VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

ZAVEDENÍ MANAGEMENTU BEZPEČNOSTI ICT NA ZÁKLADNÍ ŠKOLE

ICT SECURITY MANAGEMENT IMPLEMENTATION IN THE BASIC SCHOOL

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. JAN MATUSÍK
AUTHOR

VEDOUCÍ PRÁCE — Ing. VIKTOR ONDRÁK, Ph.D.
SUPERVISOR

BRNO 2015

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2014/2015
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Matusík Jan, Bc.

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Zavedení managementu bezpečnosti ICT na základní škole

v anglickém jazyce:

ICT Security Management Implementation in the Basic School

Pokyny pro vypracování:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

ČSN ISO/IEC 27001:2006 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky. Český normalizační institut, 2006.
ČSN ISO/IEC 27002:2005 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací. Český normalizační institut, 2005.
DOBDA L. Ochrana dat v informačních systémech. Praha: Grada Publishing, 1998. ISBN 80-716-9479-7.
DOUCEK P., L. NOVÁK a V. SVATÁ Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.
POŽÁR J. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.
POŽÁR J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

Vedoucí diplomové práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2014/2015.

L.S.

doc. RNDr. Bedřich Půža, CSc. Ředitel ústavu	doc. Ing. et Ing. Stanislav Škapa, Ph.D. Děkan fakulty

V Brně, dne 28.2.2015

Abstrakt

Obsahem této diplomové práce je návrh zavedení managementu bezpečnosti ICT na konkrétní základní škole. Úvodní část popisuje objekt školy, její vybavení a dosavadní management bezpečnosti. V praktické části jsou diskutovány nedostatky a jsou navrženy opatření pro řešení nejzávažnějších problémů školy z pohledu managementu bezpečnosti ICT.

Abstract

The aim of this study is aproposal of ICT Security Management implementation in a specific Basic school. Introduction describes the school building, its equipment and existing Security Management. The practical part consists of a discussion about current shortcomings and proposed set of measures for solving the most important problems in terms of management of ICT security.

Klíčová slova

Management bezpečnosti, bezpečnost, NAS, ICT, ISO/IEC 27000, analýza rizik

Key Words

Security management, security, NAS, ICT, ISO/IEC 27000, risk analysis

Bibliografická citace mé práce

MATUSÍK, J. *Zavedení managementu bezpečnosti ICT na základní škole.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2015. 88 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D..

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 31. května 2015

……..

Jan Matusík

Poděkování

Na tomto místě bych rád poděkoval vedoucímu své diplomové práce panu Ing. Viktoru Ondrákovi, Ph.D., za čas, který mi věnoval a ochotu při vedení mé diplomové práce. Dále bych rád poděkoval panu Ing. Petru Sedlákovi za cenné rady, trpělivost a motivaci při tvorbě diplomové práce. V poslední řadě bych rád poděkoval rodině a přátelům za motivaci a podporu při studiu.

OBSAH

ÚVOD

V době 21. století se staly informační technologie nedílnou součástí našeho života. Informační technologie nás provází každodenním životem, ať už si to připouštíme či nikoli. Díky technologiím, které v dnešní době používáme, se stáváme terčem nejen marketingových společností, které nám vnucují jejich produkty, ale také obětí kriminality, která se v oblasti informačních technologií vyskytuje v nemalém měřítku a množství.

Musíme si uvědomit, že v oblasti informačních technologií se za největší bohatství považují informace. Informace, ze kterých plynou peníze. To je důvod, proč by si lidé měli uvědomit, co sdílí, umisťují na sociální sítě a internet vůbec. Nebudeme-li si chránit data, stanou se z nás pouze oběti těch, kteří si své informace uchránili a nebáli se použít cizí k vlastnímu obohacení.

To je důvod, proč bychom se měli zamyslet nad tím, že prevence vůči takovému chování nám neuškodí. Musíme si uvědomit, že dodržování pravidel je užitečné a v případě požadavku na zachování soukromí také nezbytné.

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Cílem této práce je návrh a zavedení managementu bezpečnosti ICT na základní škole, který má vést ke zlepšení fungování a zvýšení bezpečnosti v celé organizaci. Pro toto zavedení nejsou požadovány veškeré náležitosti dané normou ISO/IEC 27001, které jsou nutné pro certifikaci. V tomto případě má norma sloužit pouze jako vodítko pro zlepšení existující situace informační bezpečnosti ve vybrané organizaci.

1 TEORETICKÁ VÝCHODISKA PRÁCE

1.1 Vymezení základních pojmů

Management

Do češtiny se management překládá jako řízení. Management jako takový umožňuje propojit činnosti různých lidí tak, aby bylo dosaženo vytyčených cílů (1, str. 13).

Bezpečnost

Bezpečnost je aktuální stav zajištěné stability, funkčnosti a existence bezpečnostních aktiv v podmínkách jak reálného tak potencionálního narušení bezpečnostními hrozbami (2, str. 33).

Hrozba

Hrozba je potencionální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace. Je to zneužití slabého místa. Pro použití v praxi, lze hrozbu definovat jako pravděpodobnost útoku odvozenou z atraktivity systému pro útočníka (3, str. 5).

Management bezpečnosti ICT

Tento pojem lze do češtiny přeložit jako řízení bezpečnosti informačních a telekomunikačních technologií. Management bezpečnosti ICT podává ucelený náhled na bezpečnostní prvky použité v organizaci (4, str. 12).

Aktivum

Aktiva jsou zdroje organizace (HW, SW, služby a informace), které mají být chráněny za pomoci bezpečnostních opatření (4, str. 346).

Dostupnost

Schopnost hardwaru, softwaru, nebo služby IT provádět dohodnutou funkci v době, kdy je požadována. Dostupnost je určována ze spolehlivosti, udržovatelnosti,

servisovatelnosti, výkonnosti a bezpečnosti. Dostupnost je zpravidla vypočítávána jako procentní podíl (5, str. 4).

Důvěryhodnost

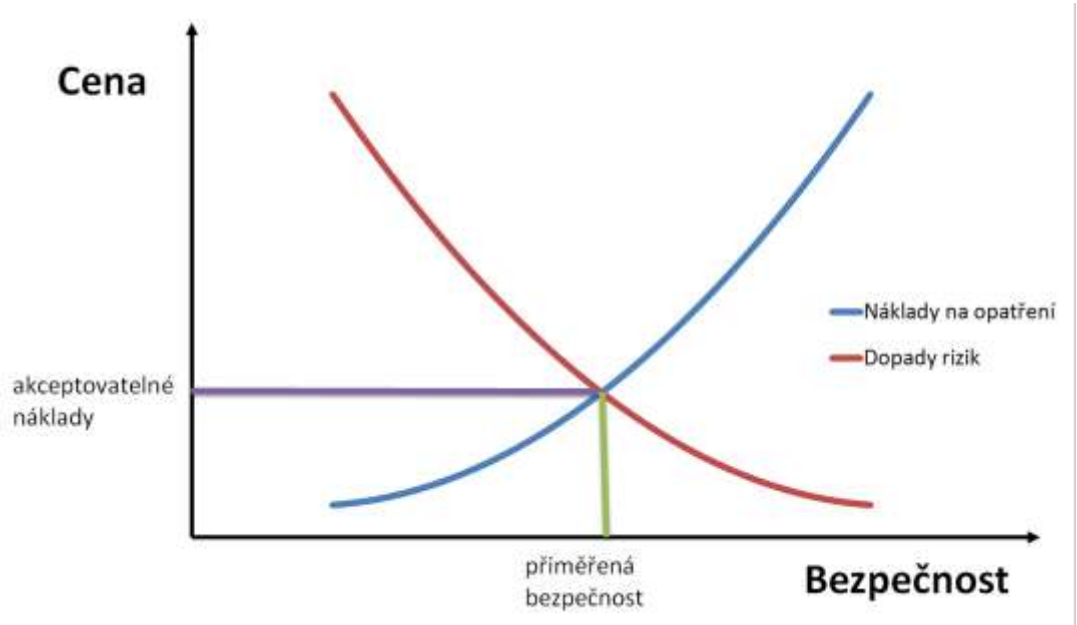
Bezpečnostní princip, jenž vyžaduje, aby data byla dostupná pouze pro autorizované osoby (5, str. 12).

Integrita

Bezpečnostní princip, který zajišťuje, že data a konfigurační položky jsou modifikovány pouze oprávněným personálem a činnostmi. Za porušení integrity se pouvažují všechny možné příčiny modifikace, včetně softwarových či hardwarových poruch, živelných událostí a lidských zásahů (5, str. 24).

1.2 Přiměřená bezpečnost

Při zavádění jakýchkoliv směrnic a bezpečnostních opatření je zapotřebí brát v úvahu přiměřenou bezpečnost. To znamená, že velikost úsilí a investic do bezpečnosti musí odpovídat hodnotě aktiv a míře možných rizik podniku. Grafické znázornění přiměřené bezpečnosti ukazuje obrázek číslo 1.



Obr. č. 1: Grafické znázornění přiměřené bezpečnosti za akceptovatelné náklady
(Zdroj: Vlastní zpracování podle (4, str. 36))

1.3 Analýza rizik

Pojem **riziko** je spojen s pravděpodobností, nebo možností škody. Jinak lze také říci, že je to očekávaná hodnota škody. Je to výsledek aktivace určitého nebezpečí, vyústěné v určitý negativní následek, neboli škodu (6, str. 2).

Analýza rizik je v procesu zavedení ISMS a zavedení managementu informační bezpečnosti velmi důležitá. Tato analýza poukazuje na aktiva, která jsou pro organizaci důležitá ve smyslu jejího fungování a celkové existence. Není použita pouze ve fázi prevence předcházení nežádoucích událostí, ale také při vlastním zásahu.

Analýzu rizik lze rozdělit do několika částí:

1. Analýza – identifikace aktiv.
2. Analýza – identifikace nebezpečí.
3. Stanovení rizika.
4. Rozhodnutí, zda je riziko přijatelné.
5. Příprava nápravných opatření, které mají za následek snížení rizika.
6. Posouzení zda plán nápravných opatření je odpovídající (6, str. 4).

Jednotlivé části 1 – 4 jsou popsány níže.

1. Analýza – identifikace aktiv

Za klíčová aktiva při analýze rizik se považují:

- Činnost v prostředí.
- Zdroje pro zajištění činnosti zvoleného prostředí.
- Nezbytná materiální i nemateriální aktiva ve zvoleném prostředí.
- Jiné nechráněné zájmy v prostředí (2, str. 19).

Příklady konkrétních aktiv jsou uvedeny v tabulce číslo 1.

Tab. č. 1: Příklad aktiv organizace z pohledu informačního systému a z pohledu firmy

Bezpečnostní aktiva	Firma	Informační systém
Zdroje	finanční zdroje	finanční zdroje
	lidské zdroje	lidské zdroje
	majetek a infrastruktura	komunikační infrastruktura
Procesy, činnosti a vztahy	produkční schopnosti	aplikační schopnosti
	správní schopnosti	systémové schopnosti
Materiální i nemateriální hodnoty	majetek movitý	hardware
	majetek nemovitý	software
	know how	data
Chráněné zájmy	kritická infrastruktura	bezpečnost systému
	obchodní tajemství	flexibilita systému

(Zdroj: Vlastní zpracování podle (2, str. 19)

2. Analýza – identifikace nebezpečí

Identifikace všech závažných zdrojů nebezpečí vztahujících se k prováděným činnostem. Je důležité zvážit, kdo, co, kdy, kde a jak může být poškozeno. Sestavení seznamu identifikace rizik může proběhnout metodou brain storming, metodou odborné konzultace, nebo za pomocí kontrolních seznamů, které jsou dostupné například v normě ČNS ISO/IEC 27005:2009 (6, str. 4).

3. Stanovení rizik

Posouzení pravděpodobnosti a následku pro každou nebezpečnou situaci nebo zdroj nebezpečí. Toto posouzení záleží většinou na zkušenostech hodnotitele a jeho osobním pohledu na věc (6, str. 4).

4. Rozhodnutí, zda je riziko přijatelné

Za pomoci předchozích kroků, je vyhodnocena závažnost rizika pro danou organizaci a je – li zapotřebí, učiní se rozhodnutí o zavedení konkrétních opatření.

Mezi hlavní přínosy analýzy rizik patří:

- Komplexní přehled o stavu informační bezpečnosti organizace.
- Návrh konkrétních opatření k nápravě zajištěných nedostatků členěných podle priorit realizace.

1.3.1 Maticová metoda analýzy rizika

Maticová metoda je jednou ze základních metod analýzy rizik využívající matici aktiv, hrozeb a zranitelností. Prvním krokem pro vytvoření matice zranitelnosti je spojení tabulky hodnocení aktiv a tabulky hrozeb a zranitelnosti. Druhým krokem je posouzení zranitelnosti jednotlivých aktiv a doplnění do matice. Třetím krokem je výpočet míry rizika za pomoci vztahu uvedeného níže (4, str. 268).

$$\boldsymbol{R = T \cdot A \cdot V}$$

R – míra rizika

T – pravděpodobnost vzniku hrozby

A – hodnota aktiva

V – zranitelnost aktiva

Posledním krokem je stanovení hranic rizika. To lze udělat za pomoci čísel či barevné škály.

1.3.2 Hodnocení rizika

Bezvýznamné, zanedbatelné riziko – nejsou zde vyžadována žádná zvláštní opatření. Nejedná se ovšem o 100% bezpečnost, proto je nutno na existující riziko upozornit a uvést např. jaká organizační a výchovná opatření je třeba realizovat (6, str. 5).

Akceptovatelné, méně významné riziko – je nutné zvážit náklady na případné řešení nebo zlepšení. V případě, že se nepodaří provést technická bezpečnostní opatření ke snížení rizika, je zapotřebí zavést vhodná opatření organizačního charakteru (6, str. 5).

Nežádoucí riziko – i když není urgentnost opatření tak závažná, jako u rizik významných, je zde zapotřebí realizovat pravidla bezpečnostního opatření dle

zpracovaného plánu, podle rozhodnutí vedení podniku. Prostředky na snížení rizika musí být implementovány ve stanoveném časovém období (6, str. 5).

Významné riziko – vyžaduje urychlené provedení odpovídajících bezpečnostních opatření snižujících riziko na přijatelnou úroveň. Je zapotřebí počítat, že na snížení rizika budou spotřebovány zdroje organizace (6, str. 5).

Nepřijatelné riziko – neboli riziko s katastrofickými důsledky, vyžadující okamžité zastavení činnosti, odstavení z provozu do doby realizace nezbytných opatření a nového vyhodnocení rizik (6, str. 5).

1.3.3 Způsoby snižování rizika

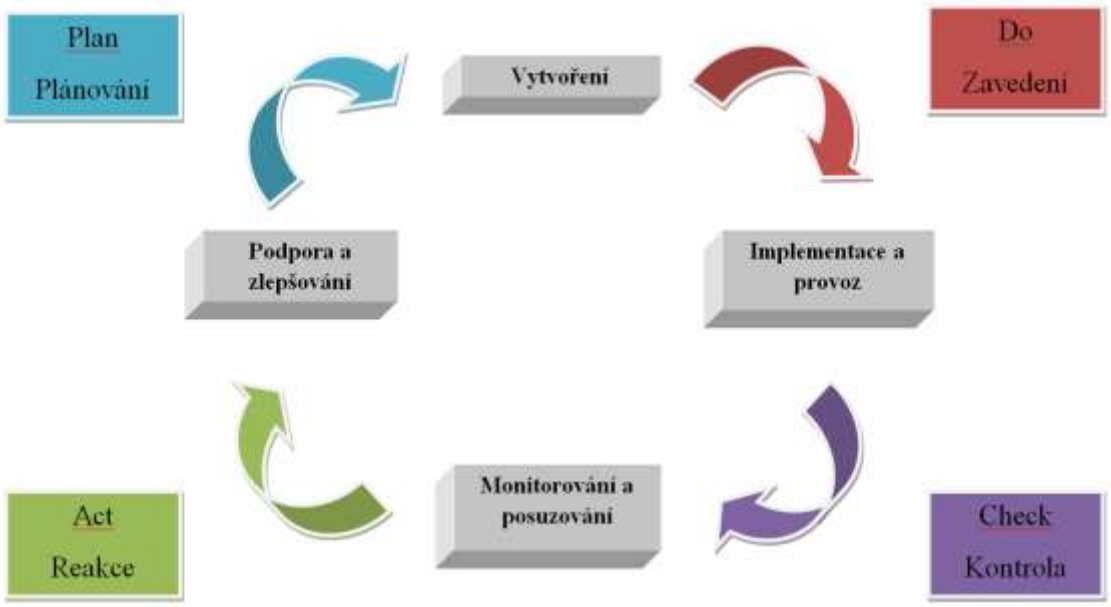
Mezi způsoby snižování rizika řadíme například:

- redukce rizik,
- retence rizik,
- přesun rizika,
- diverzifikace rizika,
- pojištění,
- vyhýbání se rizikům,
- vytváření rezerv.

1.4 Demingův cyklus

Demingův cyklus, neboli PDCA cyklus je metodou postupného zlepšování. Tato metoda se používá v realizační části zavádění managementu ICT. Dále tuto metodu můžeme nalézt například v projektovém managementu, při zlepšování jakosti produktů, služeb, aplikací, či zkvalitňování dat (7, str. 13).

Písmeno P zde znamená – fázi plánování (**P**lan), D – fázi realizace (**D**o), C – fázi přezkoumávání (**C**heck), A – fázi reakce na dané změny (**A**ct). Obrázek níže znázorňuje grafickou podobu tohoto cyklu (7, str. 14).



Obr. č. 2: Grafické znázornění Demingova cyklu (Zdroj: vlastní zpracování podle (7, str. 6))

1.5 ISMS

Definice pojmu ISMS jako takového vychází ze samotného anglického názvu Information Security Management System, což lze přeložit jako Systém řízení bezpečnosti informací. ISMS je částí celkového systému řízení organizace (4, str. 14).

ISMS využívá modelu Demingova cyklu a má 4 etapy:

- Ustanovení ISMS (určuje rozsah a odpovědnost).
- Zavádění a provoz ISMS (prosazení vybraných bezpečnostních opatření).

- Monitorování a přezkoumání ISMS (hodnocení řízení a zajištění zpětné vazby).
- Údržba a zlepšování (odstranění zjištěných slabin a soustavné zlepšování) (4, str. 14).

Rozsah ISMS je definován následujícím rozdělením aktiv:

- Informační aktiva (informace, data).
- Hardwarová aktiva (technické prostředky – hardware).
- Softwarová aktiva (technické prostředky).
- Služby poskytované prostřednictvím informačních systémů (8).

1.6 Směrnice a procesy

Směrnice a proces jsou obecné pojmy, které stanovují pravidla pro postupný tok dějů, stavů, aktivit nebo práce. Je zapotřebí je pravidelně dokumentovat a udržovat v aktuální verzi. Dokumentací je myšlen každý písemný, obrazový, zvukový, elektronický, nebo jiný záznam, ať již v podobě analogové či digitální, který vznikl z činnosti původce (5).

Revizí a analýzou firemních bezpečnostních politik lze identifikovat konkrétní zranitelná místa, která se nachází u analyzovaného subjektu. Všeobecně jsou vymezeny do čtyř sektorů.

- Fyzická bezpečnost organizace.
- Personální bezpečnost organizace.
- Informační bezpečnost organizace.
- Provozní bezpečnost organizace (2, str. 129).

1.7 Metodiky a normy ICT

Nezbytným předpokladem pro koncept řízení informatiky a informační bezpečnosti vůbec, je podpora ve formě různých standardů, nejlepších zkušeností, metodik a norem (3, str. 42).

Metodiky a normy lze chápat jako doporučení, k dosažení kýženého stavu. Nelze je tedy brát jako směrnice, které pevně vymezují hranice. Norma je požadavek na chování

systému, nebo vlastnosti věci, člověka, situace apod., který buď předepisuje a vyžaduje, nebo popisuje, co je normální (přijatelné nebo obvyklé). Norma může mít formu jak psanou tak nepsanou a liší se pouze mírou závaznosti a různým rozsahem platnosti (9, str. 9).

1.7.1 ITIL

ITIL samotný není metodikou. ITIL představuje soubor 11 knih, které obsahují popis způsobů procesního řízení služeb včetně infrastruktury IT, které jsou jejím prostřednictvím poskytovány. Cílem je poskytnutí ucelených takzvaných nejlepších zkušeností a praktik pro oblast řízení služeb IT a souvisejících procesů (3, str. 48).

1.7.2 COBIT

Jedná se o sadu všeobecně přijímaných procesů, návodů pro hodnocení, ukazatelů a nejlepších praktických zkušeností, které mají za cíl pomoci organizaci maximalizovat užitek z informačních technologií (3, str. 42).

1.7.3 Normy z řady 27 000

V následující kapitole budou popsány základní normy z řady ISO 27 000, které popisují zavádění informační bezpečnosti.

1.7.3.1 Normy specifikující požadavky

- *27001 – Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky*

Účelem je poskytnout normativní požadavky na vývoj a provoz ISMS, včetně sady opatření pro řízení a zmírnění rizik spojených s informačními aktivy, které se zvolená organizace snaží chránit (10, str. 25).

- *27006 – Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systému řízení bezpečnosti informací*

Účelem této normy je poskytnout doplnění ISO/IEC 17021 uvedením požadavků, na jejichž základě jsou certifikační organizace akreditovány. Tímto dovoluje organizacím poskytovat certifikace shody v souladu s požadavky uvedenými v ISO/IEC 27001 (10, str. 25).

1.7.3.2 Normy popisující obecné směrnice

- *27000 – Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník*

Tato norma poskytuje přehled systémů řízení bezpečnosti informací a definuje související termíny (10, str. 6).

- *27002 – Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti*

V této normě se nachází návod pro implementaci opatření bezpečnosti informací. Konkrétně je popisují kapitoly 5 až 18, které poskytují specifická implementační doporučení a návod na použití doporučených postupů podporujících opatření specifikovaných v normě ISO/IEC 27001 (10, str. 25).

- *27003 – Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systému řízení bezpečnosti informací*

Obsahem je procesně orientovaný přístup k úspěšné implementaci ISMS podle normy ISO/IEC 27001 (10, str. 25).

- *27004 – Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Měření*

Účelem této normy je poskytnutí uceleného rámce měření, umožňující posoudit efektivnost ISMS měřenou podle ISO/IEC 27001(10, str. 26).

- *27005 – Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací*

Norma poskytuje návod pro implementaci procesně orientovaného přístupu k řízení rizik, aby tak pomohla uspokojivě implementovat a splnit požadavky na řízení rizik bezpečnosti informací uvedené v ISO/IEC 27001 (10, str. 26).

- *27007 – Informační technologie – Bezpečnostní techniky – Směrnice pro auditovaní systémů řízení bezpečnosti informací*

V této normě je poskytnut návod organizacím, které potřebují provádět interní, nebo externí audity ISMS, nebo řídit program auditu ISMS na základě požadavků specifikovaným v ISO/IEC 27001 (10, str. 25).

1.7.3.3 Historický vývoj ISO/IEC 27 000

Sjednocenému standardu norem z řady ISO/IEC 27 000 předcházel dlouhý vývoj. Tento vývoj je přehledně vyobrazen na obrázku číslo 3.

Rok	Slovník	Požadavky	Soubor postupů	Implementace	Měření	Řízení rizik	Certifikace	Audit
1995			BS 7799					
1996	ISO/IEC TR 13335-1							
1997	ISO/IEC TR 13335-2							
1998						ISO/IEC TR 13335 - 3	e:cure	
1999		BS 7799 - 2	BS 7799 - 1				EA7/03	
2000			ISO/IEC 17799			ISO/IEC TR 13335 - 4		
2001						ISO/IEC TR 13335 - 5		
2002		BS 7799 - 2 v2						
2004	ISO/IEC 13335-1							
2005		ISO/IEC 27001	ISO/IEC 17799 v2					
2006						BS 7799 - 3		
2007			ISO/IEC 27002				ISO/IEC 27006	
2008						ISO/IEC 27005		
2009	ISO/IEC 27000							
2010				ISO/IEC 27003	ISO/IEC 27004			
2011						ISO/IEC 27005 v2		ISO/IEC 27007
2012		ISO/IEC 27001 v2	ISO/IEC 27002 v2					ISO/IEC TR 27008
2013	ISO/IEC 27000 v2						ISO/IEC 27006 v2	

Obr. č. 3: Vývoj norem ISO/IEC 27000 (3, str. 76)

1.8 Model OSI a jeho zabezpečení

Mezi dnes používanými síťovými modely je model OSI (Open Systems Interconnection) ten nejdůležitější. Rozděluje síťovou komunikaci do 7 vrstev a zavádí používání těchto vrstev v procesu výměny dat. Každá vrstva v průběhu odesílání dat obaluje data dalšími informacemi, naopak v případě přijetí se data zase odebírají. První 3 vrstvy mají charakter hardwaru, ostatní softwaru (11, str. 45).

Síťový model OSI je ukázán na obrázku číslo 4.

Obr. č. 4: Síťový OSI model (Zdroj: Vlastní zpracování podle (12))

1.8.1 Fyzická vrstva

Z pohledu OSI modelu leží fyzická vrstva na nejnižší úrovni. Tato vrstva definuje přenosové médium a jeho použití. Jako příklad lze uvést kabely, rádiové vlny, optická vlákna, konektory, přípojné boxy nebo rozvodné patch panely v datovém rozvaděči (11, str. 50).

Komplexní řešení bezpečnosti na této úrovni se definuje ve třech úrovních:

Bezpečnost nultého stupně (identifikační opatření) – tento stupeň nezajišťuje žádnou fyzickou ochranu komunikace, pouze usnadňuje a pomáhá správci systému určit správný způsob zapojení. Jako základní identifikační prvky zde můžeme zmínit barevné propojovací kabely, nebo barevné značkovací kroužky (4, str. 168).

Bezpečnost prvního stupně (blokační opatření) – do tohoto stupně jsou zařazeny prostředky, které chrání nebo blokují prvky kabeláže a konektivity. Mohou zde patřit

žlaby, které chrání kabely před cizím narušením, blokátory portů, nebo blokátory konektorů (4, str. 168).

Bezpečnost druhého stupně (opatření za pomoci klíčování) – do tohoto stupně se řadí prostředky, které znemožňují připojení konektorů do nepovolených portů. Může se jednat o metalické propojovací kabely, popřípadě o optické duplexní kabely (4, str. 169).

1.8.2 Linková vrstva

Na této vrstvě se realizuje přepínání ethernetových rámců. Jinak řečeno shlukují se zde datové bity proudící po fyzické vrstvě sítě a následně jsou uvedeny do kontextu spojení ve smyslu síťové trasy mezi vysílacím a přijímacím systémem (13, str. 344).

Služby poskytující linkovou vrstvou:

- tvorba rámců,
- přístup k lince,
- spolehlivost doručování,
- detekce a korekce chyb (13, str. 436).

Na této vrstvě pracují zařízení typu switch. Zabezpečení zde může probíhat:

- Za pomoci digitálního podpisu.
- Mechanismem autentizace, autorizace, audit.
- Aplikace bezpečnostních protokolů (4, str. 166).

1.8.3 Síťová vrstva

Tato vrstva poskytuje funkci řízení a směrování pro určení trasy datových paketů cestujících mezi jednotlivými sítěmi. Na této vrstvě se nacházejí zařízení typu router, popřípadě L3 switch. Zabezpečení na této vrstvě je řešeno:

- VPN,
- Systémem IDS a IPS,
- Zařízením typu firewall (4, str. 167).

1.8.4 Transportní vrstva

Transportní vrstva propojuje síťovou a relační vrstvu. Účelem této vrstvy je členění dat náležících ke konkrétní relaci a předání dat ve správné velikosti a formátu síťové vrstvy. Přechází-li data ze síťové vrstvy do relační je její odpovědností zajistit konkrétní seřazení přijatých paketů, rekonstrukci relačních informací a potvrzení přijetí. Na této vrstvě se rozpoznává, spojované a nespojované zasílání dat (11, str. 51).

1.8.5 Relační vrstva

Koordinuje komunikaci a udržuje relaci tak dlouho, dokud je potřebná. Základními prvky relační vrstvy jsou bezpečnostní mechanizmy, jako například přihlašování k relaci a další podoby dialogu s uživatelem (11, str. 52).

1.8.6 Prezentační vrstva

Na úrovni této vrstvy probíhá formátování, volitelná komprese a šifrování dat z aplikační vrstvy, data jsou dále předány vrstvě relační (11, str. 52).

1.8.7 Aplikační vrstva

V této vrstvě pracuje software, s nímž je v přímé interakci koncový uživatel. Můžeme zde zařadit například webové prohlížeče, řádková rozhraní (CLI), emailové klienty, kancelářské balíky popřípadě různé verze online Messengeru. Na této vrstvě funguje celá řada známých síťových protokolů jmenovitě například: HTTPS (Hyper Text Transfer Protocol Secure), FTP (File Transfer Protocol) nebo SMTP (Simple Mail Transfer Protocol) (13, str. 86).

Bezpečnostní prvky:

- autentizace,
- autorizace,
- Session Management,
- validace vstupů a kódování,
- ochrana dat,
- řízení chyb,
- sběr a vyhodnocení auditních informací,
- bezpečnost administrativního rozhraní.

- kryptografická ochrana.
- ochrana před známými a specifickými útoky.
- konfigurace infrastruktury (4, str. 175).

1.9 Škodlivý software

1.9.1 Malware

Malware slouží k infiltraci nebo poškození počítačového systému, bez vědomí nebo souhlasu vlastníka. Různé druhy malwaru, škodlivého kódu, se projevují různými způsoby (4, str. 349).

V následujících odstavcích budou popsány nejčastější druhy malwaru.

VIRUS – v oblasti počítačové bezpečnosti se virem označuje škodlivý program, který se dokáže často sám šířit a také modifikovat bez vědomí uživatele. Vkládá se do jiných spustitelných souborů, nebo dokumentů. Viry mohou svou činností způsobit ztrátu dat, poškození systému, nebo další šíření škodlivých virů (14).

BACKDOOR – Útočníci si na daném počítači vytvoří prostředí pro pozdější přístup. Doslova si vytvoří zadní vrátka, aby se mohli (vzdáleně a automatizovaně) k počítači nepozorovaně přihlásit (15).

ROOTKIT – Zamaskování přítomnosti škodlivého software (maskování změn v registrech, v procesech, zvýšené síťové aktivity), který pak není jednoduše odhalitelný, útočník zůstává skrytý (15).

ADWARE – Změna chování systému, především internetových prohlížečů (Internet Exploreru, Firefox, Chrome, atd.), které běží pomaleji, odkazují na jiné stránky, než které požadujeme, mění domovské stránky, mění položky v seznamu oblíbených odkazů a obtěžují s cílenou reklamou (15).

HOAX – Jedná se o falešné, poplašné a řetězové zprávy, které mají varovný/naléhavý charakter - "Rychle tuto zprávu přepošli známým, jinak…“, „Nikdy neotvírejte tento soubor, jinak…“(15).

PHISHING – Snaha podvodníků získat citlivé údaje. Útočníci tak můžou zjistit například přihlašovací údaje k různým účtům, údaje o platebních kartách, nebo získat přístup ke službám, penězům, zařízením, fotkám, atd. Typickým útokem tohoto typu je napodobení stránek online bankovnictví, kde uživatelé zadají jejich přihlašovací hesla, která nevědomě pošlou útočníkovi (15).

SPYWARE – Doslova špionážní software. Získávání citlivých informací – čísel bankovních účtů, přihlašovacích údajů, seznamů navštívených stránek a nainstalovaných programů (15).

TRACKING COOKIE – Monitorování pohybu uživatele po internetu.

BOTNET/BOT/ZOMBIE – Počítač se stane součástí řízené sítě počítačů. Např. v jeden okamžik všechny takovéto počítače zaútočí na vybraný server/službu. Z počítače se také může začít rozesílat tisíce nevyžádaných emailových zpráv za hodinu (15).

SCAREWARE – jedná se o falešný software, který se tváří/podbízí jako legitimní bezpečnostní řešení. Může se jednat například o falešné antiviry, nebo firewally (15).

TROJSKÝ KŮŇ – počítačové programy, které vypadají užitečně, nicméně mají navíc škodlivou „funkci“ (15).

1.10 Zálohování

Zálohováním rozumíme vytváření bezpečnostní kopie dat, nebo celého operačního systému, na jiném datovém nosiči, nebo místě. Zálohování provádíme, abychom byli schopni v případě havárie některé součásti počítače obnovit, stav těsně před vznikem havárie (4, str. 327).

Rozlišujeme tři základní metody zálohování:

- **Úplná záloha**

Úplnou zálohou je myšlena přesná kopie zálohovaných dat. Každá záloha je samostatná a úplně nezávislá na předchozí. Hlavní nevýhodou tohoto zálohování je potřebné místo.

- **Inkrementální záloha (přírůstková)**

Česky nazývaná přírůstková metoda. Tato metoda dovoluje zálohovat pouze soubory změněné od poslední úplné či přírůstkové zálohy. Tato metoda označuje data jako zálohované. Výhodou je zkrácená doba zálohování, je však kompenzována složitější obnovou dat. Musíme mít k dispozici úplnou zálohu a všechny přírůstkové, aby bylo vše možné obnovit (4, str. 330).

- **Diferenční záloha (rozdílová)**

Tato metoda dovoluje zálohovat pouze soubory změněné od poslední normální (úplné) či přírůstkové zálohy. Od předchozích způsobů se liší v tom, že pro obnovu potřebujeme poslední plnou zálohu, polední přírůstkovou a všechny rozdílové od poslední normální či přírůstkové (4, str. 330).

Disaster Recovery Plan

Znamená plán obnovy po havárii. Jedná se o předem připravený scénář, který vede k obnově infrastruktury po havárii. Jeho součástí je také plán zálohování.

Data lze zálohovat na:

- lokální pevný disk,
- externí a síťový disk,
- optická média,
- síťová úložiště,
- FTP server,
- pásky, nebo do virtuálního prostředí.

1.11 Network Attached Storage (NAS)

NAS je zařízení sloužící jako vyhrazené síťové úložiště, poskytující diskový prostor a služby v lokální síti. Tyto služby poskytuje přes standardní síťový protokol. Data z tohoto úložiště mohou být poskytována různým uživatelů. NAS nemusí plnit pouze funkci souborového serveru, ale může mít také specializované funkce jako P2P klient, webový server, vizualizační server, media server, nebo spousty dalších (16).

NAS obsahuje jeden a více pevných disků, které lze slučovat do větších datových struktur a vytvářet z nich RAID, který se používá jako metoda zabezpečení dat proti selhání pevného disku. Je zde však nutné podotknout že RAID nenahrazuje zálohování dat.

Nejčastěji se můžeme setkat s **RAID 0, RAID 1, RAID 5, RAID 6 a RAID 10.**

1.11.1 Zapojení diskového prostoru

1.11.1.1 RAID 0 (striping)

Není skutečný RAID, protože neobsahuje žádné redundantní informace, neposkytuje tedy uloženým datům žádnou ochranu (porucha členu znamená ztrátu dat). Jednotlivá zařízení jsou jen spojena do logického celku a vytváří tak kapacitu součtu všech členů. Jedinou výhodou této varianty je zvýšená rychlost čtení (17, str. 109).

1.11.1.2 RAID 1 (zrcadlení)

Nejjednodušší a poměrně efektivní ochrana dat. Provádí se zde zrcadlení disků. To znamená, že obsah dvou disků je naprosto stejný a v případě výpadku jednoho z disků se pracuje s druhým jako s jeho kopií. Nevýhodou tohoto nastavení je zejména rychlost zápisu a finanční náročnost při větším množství disků (17, str. 109).

1.11.1.3 RAID 5

V této konfiguraci jsou zapotřebí alespoň 3 disky, kde kapacitu jednoho disku zabírají samoopravné kódy. Tyto kódy se ukládají na jednotlivé disky střídavě a ne pouze na jeden čímž je odstraněn nedostatek RAID 4. Toto zapojení diskového pole je jednou z nejpoužívanějších variant v domácích sítích. Hlavním důvodem je, že i v případě ztráty jednoho disku jsou data stále čitelná (17, str. 109).

1.11.1.4 RAID 6

Zapojení diskového prostoru v RAID 6 je stejné jako u RAID 5 s tím rozdílem, že je zde zapotřebí minimálně 4 disků z čehož 2 disky zabírají samoopravné kódy. Jako příklad lze uvést RAID 6 s deseti disky o kapacitě 2 TB. Celková použitelná kapacita tohoto pole je 16 TB (17, str. 110).

1.11.1.5 RAID 10

Zapojení diskového prostoru v RAID 10 je kombinací RAID 1 a RAID 0 (17, str. 110).

1.11.2 Důležité pojmy – NAS

1.11.2.1 Spare disk a hot spare

Pro provoz síťových aplikací a ukládání dat je velmi důležité zachovat nepřetržitost provozu. Proto se do zařízení typu NAS vkládají takzvané spare disky. Tento disk je vložen do zařízení a není využíván až do chvíle výpadku jednoho z disků. Následně je okamžitě automaticky aktivován a jsou na něj dopočítána chybějící data za vypadlý disk. V případě, že má zařízení typu NAS přídomek hot-spare, je tím míněno, že disky lze vyměnit za provozu zařízení. V případě poruchy disku může být špatný disk vysunut a následně zasunut disk nový. To vše proběhne i v případě, že je zařízení vytíženo (17, str. 328).

1.11.2.2 Protokol SMB

Protokol SMB je součástí aplikační vrstvy. Používá se ke sdílení souborů, tiskáren, sériových portů a dalších síťových prostředků (10, str. 576).

Tento protokol poskytuje například služby typu:

- Dohodnutí protokolu mezi různými dialekty protokolu SMB.
- Zamykání souborů a záznamů.
- Oznamování změn a adresářů.
- Autentizace a autorizace přístupu k souborům, adresářům a sdíleným složkám.
- Rozšířená podpora atributů souborů.
- Síťový tisk.
- Procházení sítě nebo oznamování služeb (10, str. 577).

1.11.2.3 SAMBA

Samba je nejpoužívanějším softwarem pro sdílení souborů a tvoří základ širokého spektra produktů. SAMBA je příkladem souborového serveru s protokolem SMB.

SAMBA server lze připojit k doméně systému Windows jako souborový a tiskový server. Dokonce jej lze nainstalovat na řadič domény, kde může poskytovat souborové služby dané doméně. (10, str. 578)

SAMBA server lze nainstalovat v jednom z následujících čtyř režimů zabezpečení:

- uživatelský režim,
- sdílený režim,
- zabezpečení služby Active Directory,
- serverový režim (10, str. 579).

1.12 Řízení přístupů

V rámci oblasti ICT bezpečnosti se používá zkratka AAA, která vystihuje anglické spojení authentication, authorization and accounting. Do češtiny se tyto pojmy překládají jako autentizace, autorizace a účtování (audit) (4, str. 116).

Autentizace je důležitým pojmem v oblasti managementu ICT a bezpečnosti informací. Znamená ověření identity subjektu (osoby, systému) s požadovanou zárukou. To znamená ověření, zda je daný subjekt ten, za koho se vydává. Autentizace může být jednosměrná, obousměrná ale také průběžná. Autentizace může probíhat na základě:

- Toho **co subjekt vlastní** (například identifikační karta, identifikační dokument, šifrovaný klíč).
- Toho **co subjekt zná** (například heslo nebo identifikační frázi).
- Toho **čím subjekt je** (například biometrické údaje, jméno, otisk prstu) (9, str. 83).

Autorizace je ověření údajů při vstupu do systému či do aplikace. Předpokladem autorizace je úspěšná autentizace (9, str. 11).

Účtování (audit) slouží jako zápis výsledků z předchozích procesů (4, str. 116).

2 ANALÝZA SOUČASNÉHO STAVU

V rámci této kapitoly bude provedena analýza, která je nezbytná pro vytvoření managementu bezpečnosti. V této kapitole bude uveden popis organizace, lokality objektu a aktiv organizace týkající se informačního managementu bezpečnosti. Dále zde budou popsány směrnice a hierarchie vybrané organizace.

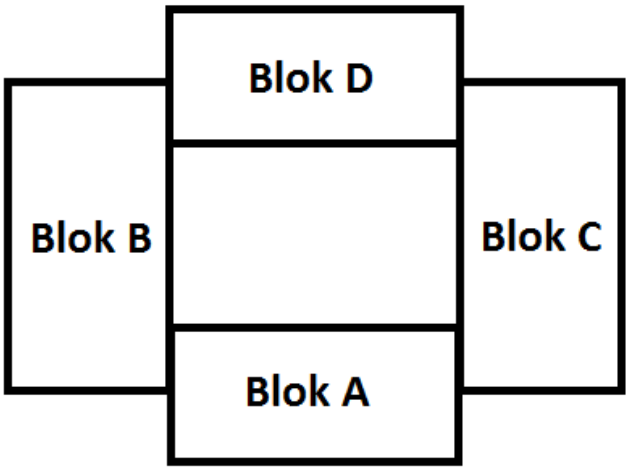
2.1 Všeobecný popis organizace

Popisovanou organizací je veřejná základní škola v Moravskoslezském kraji. Jejím zřizovatelem je město. Organizace sdružuje první a druhý stupeň základní školy, školní družinu, školní jídelnu a plaveckou školu. Všechny části školy jsou soustředěny v jedné budově.

2.2 Popis budovy

Analyzovaná škola stojí uprostřed městské panelové zástavby. Má k dispozici 23 kmenových tříd a 13 odborných učeben, z čehož 3 jsou počítačové. V objektu školy se nachází byt, ve kterém žije školník a plavecký bazén, který je součástí objektu přistavěného ke škole a je ve vyhrazených časech přístupný veřejnosti. Dále se zde nachází zázemí školní jídelny a školní družiny.

Samotnou budovu školy lze pro lepší orientaci rozdělit do 4 částí, jak lze vidět na obrázku níže.



Obr. č. 5: Schéma budovy (Zdroj: Vlastní zpracování)

V bloku budovy A se nachází ředitelství školy, odborné učebny a část tříd druhého stupně. Zbytek tříd druhého stupně je umístěn v bloku C, kde jsou také umístěny počítačové učebny. V bloku B se nachází třídy prvního stupně a školní družina. V bloku D je situována školní jídelna, tělocvičny a byt školníka.

2.3 Organizační struktura

Za chod organizace odpovídá ředitel, který se zodpovídá městu, jakožto zřizovateli školy. Ředitel má svého zástupce, který se podílí na řízení školy. Dále se v hierarchii organizace nacházejí vedoucí pracovníci jednotlivých pracovních skupin, řadoví zaměstnanci a žáci. Hierarchii školy vystihuje obrázek číslo 6.

Obr. č. 6: Grafické zobrazení hierarchie v organizaci (Zdroj: Vlastní zpracování)

V tuto chvíli organizaci navštěvuje 456 žáků, 34 učitelů a 6 vychovatelek školní družiny.

2.3.1 Analýza uživatelů

V organizaci se vyskytují 3 základní typy uživatelů:

- správci,
- zaměstnanci,
- žáci.

2.3.1.1 Správci

Nejmenší skupina ze všech. Mají v systému organizace maximální uživatelská práva a administrátorský přístup. Mají za úkol udržovat celou síťovou infrastrukturu, včetně zařízení, které do ní patří, v chodu. V tuto chvíli funkci správce zastávají 3 zaměstnanci z řad učitelského sboru a jeden externí pracovník. Správci z řad učitelského sboru jsou řadoví vyučující a činnost správce nemají smluvně přidělenu. U externího pracovníka

jde pouze o dohodu o provedení práce v určitém časovém rozsahu. Tento pracovník dostává specializované úkoly, na které správci z řad školy nemají dostatečné znalosti. Nejsou zde žádné omezení ani průběžná kontrola správců a jejich aktivit. Správci se zodpovídají řediteli organizace. Správci nepodstupují žádná pravidelná školení a v rámci smluvního vztahu s organizací nemají přiřazen status správce.

2.3.1.2 Zaměstnanci

Tato skupina uživatelů čítá zhruba 45 zaměstnanců využívajících síťovou infrastrukturu. Uživatelé mají k dispozici stolní počítače, nebo laptopy. V případě stolních počítačů využívají služby Active Directory, což znamená, že mají omezená práva. V případě laptopů se hlásí přímo do počítače jako administrátoři. Zaměstnanci využívají počítače většinou k prohlížení webového obsahu, práci s emaily a práci s aplikací Bakaláři. V případě problémů zaměstnanci kontaktují správce. Zaměstnanci nepodstupují žádná pravidelná školení, ani jinou formu vzdělávání. Je zapotřebí podotknout, že zaměstnanci nejsou obeznámeni s pravidly používání počítačů a informačních technologií v objektu školy a tedy nepodepisují ani žádnou písemnou formu těchto pravidel.

2.3.1.3 Žáci

Nejpočetnější skupina uživatelů na škole. Tato skupina se s počítači a síťovou infrastrukturou setkává především ve vyučování. Žáci se do sítě přihlašují za pomoci Active Directory a mají tedy omezená uživatelská práva. Žáci jsou obeznámeni pouze s řádem odborných učeben výpočetní techniky, který je zapotřebí přepracovat. Dále se také řídí školním řádem, který má z pohledu informační bezpečnosti rovněž nedostatky.

2.4 Analýza sítě

V následující kapitole budou analyzovány pasivní a aktivní vrstvy sítě, včetně koncových uzlů.

2.4.1 Pasivní vrstva

Pasivní vrstva komunikaci pouze zprostředkuje, ale nepodílí se na ní. V ISO/OSI modelu je pasivní vrstva brána jako fyzická.

2.4.1.1 Kabeláž

Celá datová síť je řešena pomocí nestíněných UTP kabelů kategorie 5e a 6. Podle předložené dokumentace se nejedná o certifikovaný kabelážní systém se systémovou zárukou výrobce.

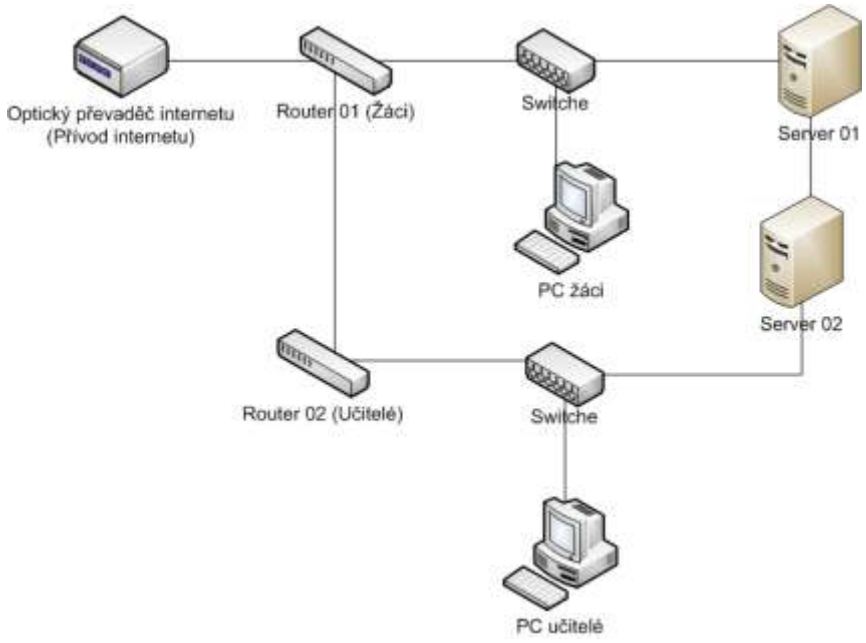
Kabeláž je po trasách ke koncovým uzlům vedena buď v chráničkách, které jsou umístěny ve zdech budovy, ve žlabech, nebo jsou umístěny volně v prostoru. Kabelážní systém neobsahuje žádnou ochranu, která by indikovala narušení kabelážního systému. Z pohledu zajištění bezpečnosti se zde nenachází žádný bezpečnostní prvek nultého, či druhého stupně.

2.4.1.2 Síťové uzly

V budově jsou umístěny 4 hlavní síťové uzly. V těchto uzlech jsou umístěny aktivní síťové prvky, které jsou vzájemně propojeny. V každém bloku je umístěn jeden z uzlů v uzamykatelné místnosti. Uzly jsou mezi sebou propojeny vždy pouze jedním kabelem, který vychází z hlavního uzlu neboli rozvaděče. Síťový uzel v bloku D slouží pouze pro aktivní prvek školníkova bytu.

2.4.2 Aktivní prvky

V rámci této kapitoly budou popsány aktivní prvky síťové infrastruktury. Pro lepší pochopení síťové infrastruktury ji obrázek číslo 7 popisuje graficky.



Obr. č. 7: Síťová infrastruktura školy (Zdroj: Vlastní zpracování)

2.4.2.1 Zařízení typu router

Organizace používá ve své síťové infrastruktuře 2 zařízení typu router. Zařízení jsou značky D -Link s označením DIR-655. Mají 1 WAN a 4 LAN porty, které jsou schopny přenášet data až 1000Mb/s . Zařízení jsou dále osazeny jedním USB portem, který se nepoužívá a který není nijak zaslepen. Zařízení také podporuje standardy sítí 802.11g/11b, avšak má odmontovány antény a funkce Wi – Fi je vypnuta. Organizace používá zařízení jako DHCP servery a oddělovače jednotlivých sítí. Na těchto zařízeních není nakonfigurován firewall ani NAT. Zařízení mají změněny přihlašovací údaje pro jejich konfiguraci. Zařízení tohoto typu jsou vhodné do domácností ne však do organizace jako je tato. Zařízení typu router nemají zaslepeny nepoužívané porty.

Obr. č. 8: Router D -Link DIR-655 (18)

2.4.2.2 Zařízení typu switch

Organizace má ve svém vlastnictví a užívání celkem 11 zařízení typu switch následujících značek a typů:

- SMC GS24C-Smart,
- TP-LINK TL-SG3424,
- D-Link DGS 1024D.

Všechny zařízení switch jsou nakonfigurovány podobně. Je u nich nastaveno pouze jméno zařízení switch, pevná IP adresa a jsou zde změněny přihlašovací údaje pro správu zařízení. Ostatní funkce zařízení switch jsou nevyužity. Volné porty zařízení switch nejsou zaslepeny. Dále budou jednotlivá zařízení popsána podle značky a typu.

- **SMC GS24C-Smart**

Organizace vlastní 3 kusy toho zařízení, je to klasický 24 portový L2 switch, který má dvacet Gigabit Ethernet portů 10BASE-T/100BASE-TX/1000Base-T a 4 Gigabit Ethernet combo porty 10BASE-T/100BASE-TX/1000BASE-T/SFP umožňující připojení k síťové infrastruktuře pomocí optického nebo metalického spojení. Nejsou zde definovány QoS pro příslušné zařízení ani aplikace. Tento switch je doporučeno používat pro domácnosti do 15 uživatelů (19).

Obr. č. 9: Switch SMC G24C-SMART (19)

- **TP-LINK TL-SG3424**

Organizace vlastní a používá 2 kusy tohoto zařízení. Jedná se o L2 manažovatelný switch, který poskytuje 24 portů 10/100/1000 Mbit/s. Switch je navíc vybaven čtyřmi sloty combo SFP. Dále je vybaven funkcemi QoS a L3, které nejsou využity.

Obr. č. 10: Swotch TP-LINK TL-SG3424 (20)

- **D-Link DGS 1024D**

Organizace vlastní a používá 6 kusů tohoto zařízení. Jedná se o klasický 24 portový 10/100/1000 Mbit/s nemanažovatelný switch. U tohoto switche nelze nastavit nic specifického, je tedy využit jeho plný potenciál.

Obr. č. 11: Switch D -Link DGS 1024D (21)

2.4.3 Koncové stanice

Ve škole se nachází 136 koncových stanic včetně 2 serverů. Tyto stanice lze rozdělit do šesti základních skupin. Prvních pět lze sloučit pod pojem **koncové stanice uživatelů:**

- stolní PC určené pro žáky,
- laptopy určené pro žáky,
- stolní PC určené pro zaměstnance,
- laptopy určené pro zaměstnance,
- volně dostupné stolní PC
- stanice typu server.

2.4.3.1.1 Koncové stanice uživatelů

Pracovní stanice jsou rozmístěny po celé škole vždy v uzamykatelných místnostech. Největší výskyt je v učebnách výpočetní techniky. Na pracovních stanicích jsou nainstalovány operační systémy Windows XP nebo Windows 7. V tuto chvíli převládá operační systém Windows XP, na který nejsou vydávány aktualizace již od 8. dubna 2014. Všechny pracovní stanice jsou (re)instalovávány manuálně včetně všech aktualizací a aplikací. Instalace dodatečných aplikací jsou spjaty pouze s konkrétním požadavkem uživatele. V celé organizaci nejsou specifikovány a definovány požadavky

nainstalované aplikace. Nejsou zde ani pravidla, která by konkrétní aplikace povolovaly, zakazovaly, či kontrolovaly stav licencí.

Všechny stanice na škole obsahují následující software:

- Kancelářský balík Microsoft Office ve verzi 2003, 2007, nebo 2013.
- AVG – Antivirový program s centrální správou.
- Přidružené služby operačního systému.
- Adobe Reader – aplikace pro čtení souborů ve formátu PDF.

Stolní počítače v učebnách navíc obsahují následující aplikace:

- Zoner Calisto 4 – vektorový grafický editor.
- Photo Studio 8 – softwarový balík určený pro práci s fotografiemi.
- Pivot Stickfigure Animator – aplikace pro vytváření animovaných postaviček a objektů, skládajících se z vybraných geometrických tvarů.
- Pinnacle Studio – nástroj pro práci s domácími videonahrávkami.

PC v užívání učitelského sboru

Učitelské počítače oproti všem ostatním obsahují pouze navíc aplikaci Bakaláři. Aplikace Bakaláři slouží jako evidence žáků a zaměstnanců, školní matrika, rozvrh hodin, rozvrh suplování a elektronická třídní kniha.

2.4.3.1.2 Servery

Škola vlastní 2 servery. Oba dva běží na systému Windows Server 2003 Standard Edition R2, který je pravidelně aktualizován. Podpora tohoto systému ze strany Microsoftu by měla být ukončena k 14. červenci 2015. Jeden ze serverů je připojen k záložnímu UPS zdroji, jehož kapacita však dostačuje při výpadku elektřiny pouze pro krátkodobý provoz v řádu minut. Oba dva servery jsou umístěny na stole v uzamykatelné místnosti, kde mají pracovnu vyučující informačních technologií. Tato místnost není vybavena klimatizací. Jsou zde dveře opatřené klikou ve tvaru koule ze strany chodby. Dále budou popsány jednotlivé servery.

Server jedna

Operační systém: MS Windows Server 2003 Standard Edition R2

CPU: Intel Pentium Dual-Core E2200; 2, 2 GHz; 1 MB L2 cache; 800 MHz FSB, socket 775

RAM: 2 GB (DDR 400 MHz)

HDD: 700GB

VGA: Intel G33 Graphics Chip Accelerator; 8 MB paměť; 8 bit sběrnice

Server má pevně nastavenou IP adresu a běží na něm následující služby:

- DNS,
- Active Directory,
- aplikace Bakaláři serverová část,
- SQL server (elektronická žákovská kniha).

Server dva

Operační systém: MS Windows Server 2003 Standard Edition R2

CPU: Intel Pentium Dual-Core E5300; 2, 6 GHz; 2 MB L2 cache; 800 MHz FSB, socket 775

RAM: 4 GB (DDR2 800 MHz)

HDD: 1 TB

VGA: Intel G33 Graphics Chip Accelerator; 8 MB paměť; 8 bit sběrnice

Server má pevně nastavenou IP adresu

Server slouží pro:

- zálohování,
- sdílení diskového prostoru.

2.5 Data a jejich klasifikace

Organizace vlastní velké množství dat jak v elektronické tak papírové podobě. Jedná se především o data osobní, tedy data značně citlivá. Elektronická verze dat není nijak kontrolována a jejich záloha nepodléhá žádné směrnici. Nyní budou uvedeny typy dat, které se v organizaci vyskytují:

- Osobní údaje o zaměstnancích, žácích a jejich rodičích.
- Výsledky studentů.
- Elektronické materiály k podpoře výuky.
- Aplikační data.
- Osobní data studentů a zaměstnanců.

2.5.1 Zálohování

V rámci organizace, neexistují žádná pravidla, ani předpisy které by určovaly co, kdy, kde a jak zálohovat. Existuje zde pouze server dva, na který jsou v nepravidelném intervalu manuálně zálohována data z aplikace Bakaláři, data učitelů a žáků, která mají uložena ve sdílených složkách. Server nemá žádnou redundanci disků, takže v případě poškození disku, bude s vysokou pravděpodobností většina dat zničena.

2.6 Autentizace, autorizace

2.6.1.1 Koncové stanice

V rámci stolních počítačů, které jsou připojené do domény, probíhá autentizace a autorizace za pomoci Active Directory, která je zprostředkována serverem jedna. Jedná se o autorizaci za pomoci uživatelského jména a hesla.

V případě autentizace a následné korektní autorizace správce, se uživatel přihlásí jako správce k lokálnímu účtu, který je vytvořen na každém PC a může zde pracovat bez omezení. V případě přihlášení obyčejného uživatele se načte účet ze serveru a uživatel má omezená oprávnění, která jsou specifikována na serveru.

U počítačů, které nejsou připojené do domény, je používána autentizace stejná jako u domény, avšak autorizace je vždy zprostředkována samotným operačním systémem.

Nejsou zde použity žádné jiné aplikace, které by ověřily, zda je uživatel ten, za koho se vydává.

2.6.1.2 Aplikace Bakaláři

V rámci aplikace jsou služby autentizace a autorizace zprostředkovávány samotnou aplikací na serveru. Uživateli je při prvním přihlášení vytvořen účet a následně při přihlášení je nucen změnit si heslo. Uživatel zde využívá znalosti uživatelského jména a hesla pro jeho ověření

2.6.1.3 Email

Emailová komunikace je přesměrovávána na osobní emaily, tudíž autentizace a autorizace je zprostředkována jednolitými servery, na kterých mají učitelé vytvořeny své emailové stránky. Většinou se jedná o servery seznam.cz, centrum.cz a google.com. Ověření uživatelů probíhá na základě uživatelského jména a hesla.

2.7 Financování

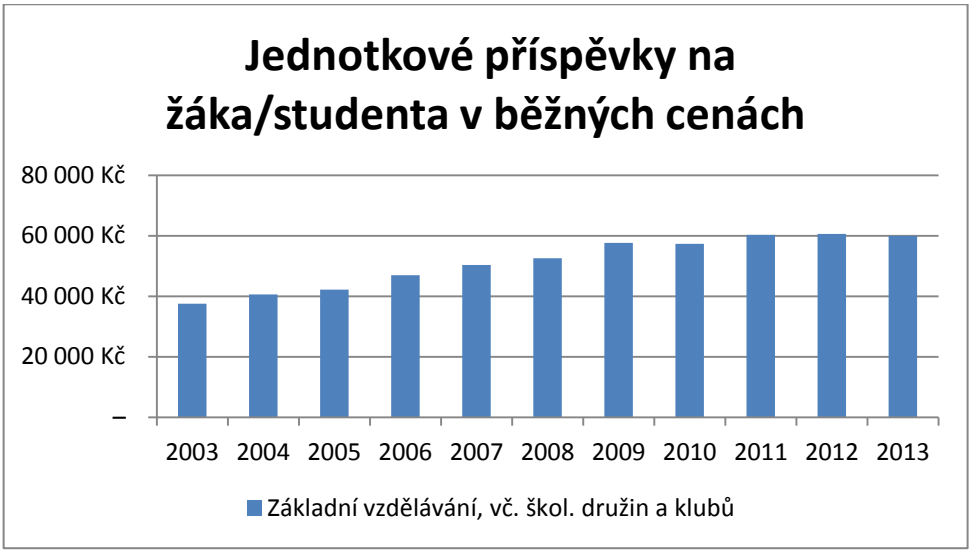
Zvolená organizace patří do veřejného sektoru školství, je tedy dotována státem. V následující tabulce číslo 2, je ukázáno kolik stát přispívá na jednoho žáka za rok. Pro srovnání financování ve školském sektoru byly v tabulce ponechány hodnoty dotací pro předškolní až vysokoškolské vzdělání. Hodnoty jsou uvedeny v rozmezí let 2003 – 2013 jako jednotkové výdaje na žáka/studenta v běžných cenách daného roku.

Tab. č. 2: Finanční příspěvky na žáka v letech 2003-2013

Rok/typ školy	Předškolní vzdělávání	Základní vzdělávání, vč. škol. družin a klubů	Střední vzdělávání a konzervatoře	Vysoké školy včetně kolejí a menz
2003	32 597 Kč	37 534 Kč	43 686 Kč	79 170 Kč
2004	33 621 Kč	40 571 Kč	44 972 Kč	82 770 Kč
2005	35 731 Kč	42 237 Kč	47 292 Kč	89 026 Kč
2006	38 924 Kč	46 962 Kč	50 515 Kč	93 538 Kč
2007	40 492 Kč	50 371 Kč	53 018 Kč	95 597 Kč
2008	41 979 Kč	52 572 Kč	54 813 Kč	93 763 Kč
2009	44 123 Kč	57 643 Kč	57 271 Kč	99 019 Kč
2010	42 477 Kč	57 293 Kč	57 010 Kč	94 454 Kč
2011	41 709 Kč	60 343 Kč	59 340 Kč	97 396 Kč
2012	43 104 Kč	60 594 Kč	63 210 Kč	99 502 Kč
2013	42 398 Kč	59 950 Kč	64 194 Kč	104 763 Kč

Zdroj: Vlastní zpracování podle (22 a 23)

V grafu číslo 1 jsou přehledně zobrazeny příspěvky státu na jednoho žáka. Lze vidět jak tyto příspěvky v průběhu let 2003 až 2010 rostly.



Graf č. 1: Příspěvky na jednoho žáka (Zdroj: Vlastní zpracováni podle (22 a 23))

Vezmeme-li v úvahu běžné náklady roku 2013 tak zvolená instituce dostala příspěvek od státu ve výši zhruba 27 337 200. Průměrný plat učitele je stanoven na částku

24 317,62 Kč. To znamená, že výdaje školy na platy zaměstnanců se za rok pohybují okolo 11,7 milionu korun (22).

Dále musíme vzít v úvahu, že škola ročně zaplatí zhruba 1,5 milionu za spotřební materiál a 2,3 milionu za spotřebované energie. Po těchto výdajích škole zbývá zhruba 11,5 milionu na fungování a opravy školy.

2.8 Analýza bezpečnosti podle ukazatelů definovaných v normě ISO 27001

V následující kapitole bude proveden audit jednotlivých politik podle ISO normy ISO/IEC 27001 přílohy A. Budou zde doplněny otázky informační bezpečnosti, které nebyly zodpovězeny v předchozích kapitolách.

2.8.1 Politika bezpečnosti informací a jejich organizace

Podle normy ISO/IEC 27001, přílohy A, bodu A.5 a A.6, ve vybrané organizaci není definována politika bezpečnosti informací a tudíž ani její organizační struktura. Nejsou zde definována ani pravidla, která by popisovala bezpečnost použití mobilních zařízení pro práci na dálku.

V organizaci nejsou definovány role odpovědnosti bezpečnosti informací ani principy oddělení povinností jednotlivých zaměstnanců.

2.8.2 Politika bezpečnosti lidských zdrojů

Podle bodu A.7 by v organizaci měla být definována pravidla bezpečnosti lidských zdrojů ve třech úrovních. Před, během a po ukončení pracovního stavu. Cílem stanovení pravidel je zajistit, aby zaměstnanci, popřípadě žáci, byli srozuměni se svými povinnostmi a aby pro jednotlivé role byli vybráni vhodní kandidáti. V tomto okamžiku organizace nevlastní žádnou směrnici, která by politiku bezpečnosti lidských zdrojů celistvě popisovala.

2.8.3 Řízení aktiv

Bod A.8 popisuje zavedení managementu řízení aktiv. Ve vybrané organizaci není nijak specificky rozvržena odpovědnost za aktiva. Jak bylo již napsáno v hierarchii organizace, za všechna aktiva odpovídá ředitel. Jednotlivým pracovníkům je sice

přidělena odpovědnost za konkrétní aktiva, nemají však tuto skutečnost nijak smluvně ošetřenou, tudíž není striktně dodržována.

Klasifikace informací a konkrétní způsob manipulace s médii rovněž není definován.

2.8.4 Řízení přístupů

Ve škole není nijak popsána problematika přístupu uživatelů, ať už jde o data, přístup do systému, či o přístupy do konkrétních prostor budovy školy.

Pro samotnou registraci/rušení uživatelských účtů nemá organizace žádný specifický proces. V případě potřeby jeden ze správců účet zruší či vytvoří. Organizace nemá žádný konkrétní systém pro správu hesel.

2.8.5 Kryptografie

V organizaci se nevyužívající žádná speciální kryptografická řešení.

2.8.6 Fyzická bezpečnost a bezpečnost prostředí

Slouží pro předcházení neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací v organizaci. V objektu školy je umístěna vrátnice, kde sedí povolaný pracovník. Tato osoba se stará o uzavírání hlavního vchodu, který slouží pro příchod a odchod žáků či cizích osob. Rovněž otevírá a uzamyká školní šatny a eviduje žáky, kteří přijdou mimo běžnou dobu příchodu do školy. Dále se stará o evidenci osob, které do školy přijdou a nejsou v přímém vztahu se školou.

Všechny kanceláře a učebny jsou opatřeny zámkem. Po ukončení vyučování jsou třídy uzamčeny do dalšího dne. Za tuto činnost ovšem není nikdo oficiálně zodpovědný.

V některých částech budovy je nainstalován alarm, který v případě spuštění přivolá policii a ředitele školy. Do budoucna je plánováno rozšíření do celého objektu školy.

Aktivní prvky organizace jsou kromě dvou zařízení typu router umístěny v uzamykatelných RACK skříních. Tyto skříně však nejsou uzamčeny a klíče jsou v zámku. RACK skříně jsou umístěny v kabinetech nebo jiných uzamykatelných místnostech. Jak bylo popsáno výše. Kabelážní systém je na některých úsecích umístěn

v chráničkách či ve zdi. Na mnohých místech jsou však kabely volně přístupné, stejně jako internetové zásuvky. Některé z těchto zásuvek nejsou aktivovány.

K problematice řízení přístupu nebyla předložena žádná další dokumentace.

2.8.7 Bezpečnost provozu

Cílem bezpečnosti provozu je zajištění správného a bezpečného provozu pro zpravování informací. V organizaci neexistují dokumenty, které by dokládaly provozní postupy, dostupné všem zaměstnancům dle aktuální potřeby. Nejsou zde nastaveny procesy pro řízení změn a kapacit, které se mohou týkat lidských zdrojů či jiných aktiv organizace.

Ochrana proti malwaru zde probíhá za pomoci aplikace AVG, která je centrálně spravována a aktualizována. Ochrana samotných dat proti ztrátě není nijak zavedena. Organizace zálohuje pouze data aplikace Bakaláři. Tato záloha probíhá manuálně v rámci 2 serverů, které jsou na škole dostupné. Zálohy nejsou nijak striktně časově nastaveny, ani procesně ošetřeny.

Síťová komunikace v rámci organizace není logována ani monitorována. Jediné logování lze nalézt v aplikaci Bakaláři, kde je tato funkce automatická.

V organizaci nejsou implementovány postupy řízení instalace a aktualizace softwaru na koncových stanicích.

2.8.8 Bezpečnost komunikace

Jak bylo uvedeno výše, síť není specificky spravována ani kontrolována, nenastane-li problém s komunikací v síti. Nastane-li tento problém, je přivolán externí pracovník, který se společně se správcem sítě podílí na řešení problému. Síť je dělena dvěma směrovači.

V tuto chvíli v organizaci není zajištěna ochrana informací přenášených při transakcích aplikačních služeb tak, aby se zabránilo neúplnému přenosu informací, neoprávněným změnám zpráv, chybnému směřování, neoprávněnému vyzrazení, duplikaci či opakovanému přenosu zprávy.

Komunikace v organizaci probíhá za pomoci emailů. Organizace však nevlastní emailový server, a tudíž využívá server třetí strany, který zprávy přímo přeposílá na soukromé emailové adresy zaměstnanců.

2.8.9 Akvizice, vývoj a údržba systému

Organizace nemá žádný ucelený informační systém, kterým by se řídila celá organizace, proto není možné popsat samotný vývoj, ani údržbu. Využívá pouze aplikace Bakaláři, který není vyvíjen školou. Aplikace jako taková je vyvíjena třetí stranou, pravidla bezpečnosti jsou tedy definována od vývojářů. Samotná třetí strana se také stará o aktualizace, které jsou distribuovány online.

2.8.10 Dodavatelské strany

Bezpečnost informací v dodavatelských vztazích není nastavena. Je zapotřebí dodat, že zaměstnanci, kteří pro školu pracují externě, nemají ve smlouvách podstatu bezpečnosti informací opatřenu. V tuto chvíli se jedná pouze o jednu osobu, která škole pravidelně pomáhá se správou sítě a aplikací. Tato osoba by však neměla mít přístup k citlivým informacím o žácích či zaměstnancích školy, které jsou uloženy v aplikaci Bakaláři a jsou zašifrovány.

Organizace má dále dodavatelské vztahy s poskytovatelem internetu, který se smluvně zavazuje, že organizaci bude dodávat internet v poměru rychlostí 26/26 Mb/s, s agregací 1:1 a jednou statickou IP. Ve smlouvě není nijak uvedeno s jakou dostupností a jaká je kompenzace v případě nedodržení závazků. Poskytovatel internetu nemá přístup do lokální sítě této organizace.

2.8.11 Řízení incidentů bezpečnosti informací

Organizace nemá žádnou dokumentaci týkající se řízení incidentů bezpečnosti informací. Jediná oficiální odpovědná osoba je ředitel, který zodpovídá za vše. Ředitel sice deleguje povinnosti na ostatní pracovníky, tyto povinnosti však nejsou nikde jasně a striktně definovány a hlavně nejsou smluvně opatřeny. Hlášení a řešení krizových situací probíhá bez plánování, za běhu celé organizace. Neexistuje zde ani dokumentace zaznamenávající ponaučení z řešení předcházejících problémů, které by byly souhrnně popsány a umístěny na jednom místě pro případné použití.

2.8.12 Aspekty řízení kontinuity činnosti organizace z hlediska bezpečnosti informací

Organizace nemá definován Disaster Recovery plán.

2.8.13 Soulad s požadavky

Organizace splňuje požadavky nutné pro provoz školy, které jsou definovány naším státem. Zcela zde chybí dokumentace, kterou stát sice nevyžaduje, ale při provozu školy by mohla značně ulehčit řešení různých situací. Jsou dodržovány práva duševního vlastnictví, ochrana osobních údajů jak zaměstnanců, tak žáků a to minimálně v papírové podobě.

2.9 Souhrn

Uživatelé jsou neznalí problematiky informační bezpečnosti a navíc nejsou řízeni v ohledu této problematiky. Vyskytují se zde problémy s dokumentací, která ve většině případů úplně chybí. Hardware, který má zabezpečovat informační provoz organizace, není dostatečně způsobilý k tomuto použití. Důvodem, je především nedostatečný výkon a zabezpečení dat. Softwarová stránka věci také není v pořádku. Nejsou zde stanoveny žádná pravidla používání softwaru a hlavně není kontrolován jeho licenční stav.

Aktuální stav týkající se bezpečnosti ICT je tedy na nízké úrovni. Budeme-li hovořit o stavu ICT jako celku musíme se bavit o mnohdy zastaralém vybavení, které funguje pouze na „dobré slovo“.

3 VLASTNÍ NÁVRHY ŘEŠENÍ

V rámci této kapitoly budou předloženy návrhy na zlepšení současného stavu, které by měly přinést zlepšení informační bezpečnosti celé organizace. Návrhy budou vycházet z ISO norem, nejlepších zkušeností a analýzy informačních rizik, která bude v této kapitole provedena.

3.1 Analýza a hodnocení rizik

V následující kapitole navrhnu a provedu analýzu aktiv a hodnocení rizik. Na základě těchto analýz doporučím změny v organizaci.

3.1.1 Identifikace aktiv

Pro zajištění základních aktiv, je zapotřebí brát v úvahu závažnost možného dopadu v případě porušení bezpečnosti. Z tohoto důvodu navrhuji klasifikační schéma pro hodnocení aktiv, které následně použiji.

Tab. č. 3: Klasifikační schéma pro hodnocení aktiv

Váha aktiva	Váha – hodnota aktiva slovně	Hodnocení dopadů
1 , 2	Zanedbatelná	Žádný, nebo zanedbatelný dopad
3	Malá	Malý dopad
4	Významná	Vážné potíže
5	Velmi cenná	Velmi vážné

(Zdroj: Vlastní zpracování)

V tabulce číslo 4 jsou uvedena aktiva, která jsou pro organizaci kritická z pohledu informační bezpečnosti. V případě nalezení dalšího aktiva tato tabulka může být kdykoliv modifikována.

Tab. č. 4: Určení váhy aktiv

Aktivum	Dostupnost	Důvěryhodnost	Integrita	Váha
Pracovní stanice	3	3	2	3
Lokální servery	5	4	4	5
Routery	5	3	3	4
Switche	2	3	3	3
Osobní data (žáci)	3	3	4	3
Osobní data (zaměstnanci)	3	3	4	3
Technická dokumentace	3	3	5	4
Elektronická pošta	2	4	5	4
Smlouvy	3	3	3	3
Databázová data	4	3	4	4
Zálohy dat	4	4	5	5

(Zdroj: Vlastní zpracování)

Položka **dostupnost** znamená, že informace je pro oprávněného uživatele přístupná v okamžiku její potřeby. **Důvěryhodnost** znamená, že je distribuce informací zajištěna pouze těm, kteří jsou k tomu oprávnění. Položka **integrita** znamená zajištění správnosti a úplnosti informací, to znamená, že informace nebudou nijak změněny. **Váha** udává hodnotu daného aktiva pro organizaci.

Tabulka číslo 5 udává, jak moc mohou daná aktiva ovlivnit chod organizace podle jejich hodnoty.

Tab. č. 5: Váha aktiv a hodnota dopadu

Váha aktiva	Hodnota dopadu na dané aktivum
Zanedbatelná	Dopad je zanedbatelný – bezvýznamné riziko • Odstranění následků proběhne bez jakéhokoliv problému v krátkém časovém horizontu, bez finanční nákladnosti • Následky se neprojeví na chodu organizace • Nebyla porušena právní legislativa
Malá	Dopad na aktiva organizace je malý – akceptovatelné riziko • Odstranění následků proběhne s malými problémy, stále však v krátkém časovém horizontu, bez finanční nákladnosti • Má negativní vliv na organizační celky působící v organizaci, ale navenek se neprojeví • Nedošlo k zásadnímu porušení právní legislativy
Významná	Dopad na aktiva organizace je vážný – mírné/nežádoucí riziko • Odstranění následků proběhne se značnými problémy, v neurčitém čase a značnou finanční nákladností • Negativní dopad na organizační celky, projeví se i navenek • Mohlo zde dojít k zásadnímu porušení právních norem • Újma způsobená jedné či více osobám mimo ohrožení zdraví či života
Velmi cenná	Dopad na aktiva organizace je velmi vážný – nežádoucí/nepřijatelné riziko • Ztráta důvěryhodnosti • Veřejná negativní publicita • Citelná finanční ztráta • Ohrožení života, či zdraví • Odstranění následků proběhne pokud možno s velkým úsilím, v dlouhém časovém horizontu • Možnost zániku školy

(Zdroj: Vlastní zpracování)

3.1.2 Identifikace hrozeb

V tuto chvíli jsou definována aktiva důležitá pro chod školy. Nyní navrhnu možné Hrozby pro tyto aktiva a určím, s jakou pravděpodobností tato hrozba může nastat.

Tabulka číslo 6 uvádí klasifikační schéma pro převod číselné hodnoty na slovní hodnocení pravděpodobnosti, že daná hrozba nastane.

Tab. č. 6: Klasifikační schéma pravděpodobnosti hrozby

Hodnota	Pravděpodobnost
1	Mizivá až žádná
2	Nízká
3	Střední
4	Vysoká
5	Velmi vysoká

(Zdroj: Vlastní zpracování podle)

V následující tabulce jsou uvedeny konkrétní hrozby s pravděpodobností.

Tab. č. 7: Tabulka hrozeb

Hrozby	Pravděpodobnost
Porucha HW	5
Selhání SW	3
Ztráta dat	4
Selhání komunikace	3
Napadení sítě	3
Neúmyslný incident	4
Živelná pohroma	2
Úmyslný incident	2
Neoprávněný přístup	4

(Zdroj: Vlastní zpracování)

3.1.3 Matice zranitelnosti

Tab. č. 8: Matice zranitelnosti

V Zranitelnost	Popis aktiva	Pracovní stanice	Lokální servery	Routery	Switche	Osobní data (žáci)	Osobní data (zaměstnanci)	Technická dokumentace	Elektronická pošta	Smlouvy	Databázová data	Zálohy dat
	Hodnota aktiva	3	5	4	2	3	3	4	4	3	4	5
Popis hrozby	Pravděpodobnost											
Porucha HW	5	3	5	4	2				4			
Selhání SW	3	2	3									
Ztráta dat	4	3	4			3	3	4	4	3	4	4
Selhání komunikace	3	2	3	3	2				3			
Napadení sítě	3	2	3	3	2				3	2	3	3
Neúmyslný incident	4	3	4	4	2	3	3	4	4	3	4	4
Živelná pohroma	2	2	2	2	1	2	2	2	2	2	2	2
Úmyslný incident	2	2	2	2	1	2	2	2	2	2	2	2
Neoprávněný přístup	4	3	4	4	2	3	3	4	4	3	4	4

(Zdroj: Vlastní zpracování)

3.1.4 Matice rizik

V následující tabulce je vyobrazena celková hodnota rizika.

Tab. č. 9: Matice rizik

R Riziko	Popis aktiva	Pracovní stanice	Lokální servery	Routery	Switche	Osobní data (žáci)	Osobní data (zaměstnanci)	Technická dokumentace	Elektronická pošta	Smlouvy	Databázová data	Zálohy dat
	Hodnota aktiva	3	5	4	2	3	3	4	4	3	4	5
Popis hrozby	Pravděpodobnost											
Porucha HW	5	45	125	80	20				20			
Selhání SW	3	18	45									
Ztráta dat	4	36	80			36	36	64	64	36	64	80
Selhání komunikace	3	18	45	36	12				36			
Napadení sítě	3	18	45	36	12				36	18	36	45
Neúmyslný incident	4	36	80	64	16	36	36	64	64	36	64	80
Živelná pohroma	2	12	20	16	4	12	12	16	16	12	16	20
Úmyslný incident	2	12	20	16	4	12	12	16	16	12	16	20
Neoprávněný přístup	4	36	80	64	16	36	36	64	64	36	64	80

(Zdroj: Vlastní zpracování)

Tab. č. 10: Klasifikační schéma pro vyhodnocení matice rizik

Hodnota rizika	Slovní vyjádření	Horizont řešení
0 -25	Bezvýznamné riziko	Není zapotřebí řešit
26-50	Akceptovatelné riziko	3 – 5 let
51-75	Mírné riziko	1 – 3 roky
76-100	Nežádoucí riziko	Do 1 roku
nad 100	Nepřijatelné riziko	Okamžitě

(Zdroj: Vlastní zpracování)

3.1.5 Zhodnocení rizik

Z analýzy rizik vyplývá, že největší riziko pro organizaci plyne z poruchy hardwaru. Dalšími riziky, kterými je zapotřebí se zabývat, je ochrana dat proti poškození, zneužití a ztrátě. Je také zapotřebí, postarat se o ochranu lokálních serverů proti neoprávněnému přístupu. V rámci následujících kapitol se budu zabývat těmito riziky a riziky s nimi spjatými.

3.2 Organizační struktura

Pro zavádění managementu bezpečnosti ICT a ISMS je velice důležitým prvkem organizační struktura. Bez zavedené a zdokumentované hierarchie organizační struktury probíhá zavádění složitě a mnohdy neúspěšně.

V rámci analyzované organizační struktury je správně nastavena hierarchie. Doporučuji tuto hierarchii zdokumentovat s jasným a striktním popisem činností, které daná funkce vykonává. Neměla by se, vyskytnout situace, že zaměstnanec vyučující informatiku bude dělat správce sítě, aniž by tuto skutečnost měl uvedenu ve smlouvě. Proto doporučuji, aby se tyto informace promítly do smluv zaměstnanců, kteří nebudou mít zodpovědnost pouze za výuku, ale budou také zodpovídat za stav majetku školy (učební pomůcky).

Jedna osoba může nabývat více funkcí, je však zapotřebí, aby vše bylo ošetřeno smluvně. To znamená, že zaměstnanec může být na půl úvazku správcem sítě a na půl úvazku učitelem. Doporučuji jasně definovat funkce:

- krizový manažer,
- bezpečnostní technik,
- CISO (manažer bezpečnosti),
- správce sítě,
- učitel, asistent, vychovatelka (řadový zaměstnanec),
- uklízečka, vrátná,
- technický pracovník (školník, správce),
- žák,
- ředitel,
- externí pracovník aj..

Doporučuji, aby se do smluv vyučujících promítly povinnosti ne jenom během pracovního vztahu, ale také před a po něm. Tím je myšleno:

- Zaměstnanec nevynese interní informace (například finanční příjmy, projektová dokumentace, specifické know-how organizace …).
- Zaměstnanec nevynese osobní informace třetích osob.
- Zaměstnanec po ukončení pracovního poměru nebude využívat přístupů, které nabyl jako zaměstnanec ať už k systémům, nebo datům organizace.

V rámci aplikace tohoto opatření, bude jasně stanovena zodpovědnost a pracovní povinnosti jednotlivých zaměstnanců organizace. Bude zde jasná orientace v celé hierarchii organizace, tudíž zde nemohou nastat rozepře v rámci identifikace odpovědnosti jednotlivých zaměstnanců. V případě vytvoření nové zaměstnanecké role bude díky dokumentaci a jasnému popisu funkcí snazší začlenit ji do struktury organizace.

3.3 Politika bezpečnosti sítě

Doporučuji zavést politiku bezpečnosti sítě. Doporučuji, aby bezpečnostní politika obsahovala minimálně dokumenty s následujícími tématy:

- Povolená zařízení v organizaci a jeho správa.
- Povolený software v organizaci a jeho správa.

- Poučení uživatelů o chování v rámci sítě organizace.
- Práci s médii a zálohování.
- Plán obnovy po havárii. (Disaster Recovery Plan)
- Odpovědnost za dokumentaci a je její dodržování.
- Dodržování managementu bezpečnosti ICT.
- Práce s osobními daty.

Některá doporučení k obsahu jednotlivých dokumentů lze nalézt v kapitolách týkajících se daného tématu.

Všechny tyto doporučení by se měly objevit ve školení pro zaměstnance a samozřejmě měly by být stvrzeny podpisem ředitele organizace a jednotlivých zaměstnanců.

3.4 Fyzická bezpečnost a bezpečnost prostředí

Následující kapitola bude popisovat doporučení, týkající se fyzické bezpečnosti a bezpečnosti prostředí.

3.4.1 Pasivní vrstva

Doporučuji v organizaci zavést management pasivní vrstvy nultého, prvního i druhého stupně. V případě nejasnosti doporučuji použít normu ČSN EN 50173-1.

3.4.1.1 Zavedení nultého stupně

Doporučuji označit – štítkovat jednotlivá síťová zařízení, patch panely a zásuvky pro jejich snadnou identifikaci a orientaci v nich. Označení aktivních zařízení doporučuji v následujícím tvaru:

Označení zařízení_Označení bloku budovy + Označení patra_Označení místnosti_Označení pozice v RACK skříni/označení koncové stanice

Označení zařízení: PC – koncová stanice, P -patch panel, S -Switch, R -Router,

Označení pavilonu: A, B, C, D

Označení patra: XX (01, 02, 03)

Označení místnosti: YYY

Označení pozice v RACK skříni: Z

Příklad:

S _B02_201_3 – jedná se o switch umístěný v bloku budovy B ve druhém patře v místnosti 201 na pozici v RACK skříni č. 3.

Síťové zásuvky doporučuji značit následovně:

Označení bloku budovy + Označení patra_Označení místnosti_Označení zásuvky_Označení portu v případě že je zde víc než jeden

Příklad:

B02_202_1 _A – jedná se o port umístěný v bloku budovy B v druhém patře, místnosti 202, zásuvka číslo 1, port A.

Dále v rámci nultého stupně doporučuji použít barevně odlišené kabely pro propojení jednotlivých aktivních zařízení. Samozřejmostí je i svazování kabelů a jejich srovnání v RACK skříni.

Doporučuji, aby měl kabel na obou stranách štítek, na kterém je uvedeno, kam je připojen. Důvodem je náhodné vytrhnutí a následná identifikace kabelu.

Na základě těchto doporučení bude mít správce sítě přehled nejen o zařízeních, která jsou v síti zapojeny, ale v případě nefunkčnosti některého ze zařízení může rychleji diagnostikovat závadu.

3.4.1.2 Zavedení prvního stupně

Doporučuji v rámci bezpečnosti a přehlednosti zaslepit porty síťových zástrček u aktivních prvků (zařízení typu switch a router) i u síťových zásuvek a patch panelů, které jsou nepoužívané a neaktivní. U nepoužívaných portů doporučuji tyto porty úplně odpojit.

Doporučuji použít blokátory datových portů RJ-45 u síťových zásuvek a koncových stanic, aby nedocházelo k neoprávněnému přepojování síťové kabeláže. Jako další krok doporučuji uschovat všechny volně uložené kabely do chrániček ve stěnách, nebo do uměle připevněných žlabů.

Dále doporučuji uzamknout všechny RACK skříně. Jednu kopii klíče pak uložit u ředitele v sejfu a druhou kopii do uzamykatelné skříně u zodpovědného pracovníka IT. V případě použití některého z klíčů, doporučuji zapsat, kdo si klíč zapůjčil, na jak dlouho a z jakého důvodu. To vše doporučuji zapsat do dokumentu, který bude u klíčů přiložen.

Tato opatření mohou zabránit poškození sítě a zneužití síťových služeb sítě nepovolanou osobou.

3.4.1.3 Zavedení druhého stupně

V rámci druhého stupně bezpečnosti doporučuji pro porty na zařízení switch, které mají pevně nakonfigurovány vlastnosti pro konkrétní zařízení, umístit speciální klíčované konektory, aby do těchto portů nemohla být náhodně připojena zařízení, které tam nepatří.

3.4.1.4 Zavedení technické dokumentace pasivní vrstvy

Doporučuji zavést dokumentaci, ve které bude přesně definováno, co a kde je připojeno. Za tento dokument by měla být zodpovědná jedna osoba, která bude dokumentovat případné změny v síti a bude zodpovědná za aktuálnost tohoto dokumentu. To znamená, že v případě zapojení nového zařízení zodpovědný pracovník zpřístupní port na aktivním prvku, propojí jej s datovou zásuvkou a s koncovým zařízením. Následně vše zdokumentuje v přehledné tabulce. Tabulku doporučuji vytvářet v následujícím tvaru:

Tab. č. 11: Dokumentace pasivní vrstvy (Zdroj: Vlastní zpracování)

Identifikátor koncové stanice	Zásuvka	Patch panel	Aktivní Prvek
PC_B02_201_01	B02_202_1_A	P_B02_201_1	S_B02_201_3_3

(Zdroj: Vlastní zpracování)

Slovní popis

Počítač číslo 1 v bloku budovy B ve druhém patře místnosti 201 je připojen do zásuvky B02_202_1_A, která je zapojena v patch panelu P_B02_201_1, který je připojen do aktivního prvku S_B02_201_3_3.

Doporučuji touto dokumentací pověřit správce sítě, který se nejčastěji stará o kabelážní systém, zařízení typu switch a router.

3.4.2 Bezpečnost prostředí

Doporučuji ustanovit v rámci pracovních povinností technických pracovníků, aby třídy po poslední vyučovací hodině byly řádně uzamčeny a odemčeny až následující den v 7 :30.

Doporučuji, aby místnosti, ve kterých jsou umístěny aktivní prvky, byly uzamčeny a opatřeny zabezpečovacím systémem a klikou ve tvaru koule. Dále doporučuji stanovit, že v místnostech s aktivními prvky mohou být vždy pouze pověřené osoby. Nikdy by zde neměl zůstat žák, návštěva či nepovolaný zaměstnanec sám.

3.4.3 Zapojení síťových uzlů

Doporučuji změnit propojení uzlů. Topologie hvězdy je v pořádku, ovšem doporučuji znásobit množství propojení mezi jednotlivými uzly. Důvodem je zlepšení propustnosti sítě a možnost vyhnutí se výpadku a nedostupnosti jednoho z uzlů v případě poškození kabelu popřípadě některého portu na aktivním prvku.

3.5 Aktivní prvky

3.5.1 Zařízení typu switch

V rámci sítě na druhé vrstvě ISO/OSI modelu doporučuji sjednotit všechna zařízení typu switch. Důvodem je nahraditelnost jednotlivých zařízení a jednodušší způsob managementu. Nedoporučuji kupovat zařízení typu D-Link DGS 1024D, které není výhodné z pohledu ceny ani výkonu. Do budoucna bych doporučil nahradit D -Link DGS 1024D switchi typu TP-LINK TL-SG3424, SMC GS24C-Smart, popřípadě jiným modelem který umí vytvářet a spravovat VLAN, popřípadě síť manažovat jiným způsobem.

V návaznosti na tento fakt doporučuji ve škole vytvořit 6 VLAN pro specifické účely. VLAN 1-VLAN 3 do které budou spadat všechny PC, které jsou v učebnách. Do VLAN 4 budou spadat všechny učitelské počítače, které jsou pevně umístěny, a není s nimi manipulováno. Do VLAN 5 budou spadat ostatní počítače (síťové zásuvky),

které se po škole přemisťují, popřípadě si je vyučující berou i domů. V poslední VLAN 6 budou umístěny servery. Pro lepší pochopení jsou data jednotlivých VLAN přeskupena do tabulky číslo 11.

Tab. č. 12: Popis jednotlivých VLAN

Název podsítě	Přibližný počet připojených PC	Rozsah síťových adres
VLAN 1	Učebna č. 1 – 29 PC	192.168.1.1-192.168.1.29
VLAN 2	Učebna č. 2 – 16 PC	192.168.2.1-192.168.2.16
VLAN 3	Učebna č. 3 – 12 PC	192.168.3.1-192.168.3.12
VLAN 4	Pevné stanice – 57 PC	192.168.40.1-192.168.40.57
VLAN 5	Pohyblivé stanice (laptopy) – PC 20	192.168.50.1-192.168.50.20
VLAN 6	Servery	192.168.60.1-192.168.60.3

(Zdroj: Vlastní zpracování)

Takto rozdělená síť může zabránit virové nákaze, popřípadě může znemožnit přístup žáků k citlivým datům. Tím je myšleno, že z VLAN 1 – VLAN 3 nebude možno přistupovat do VLAN 4 a VLAN 6.

Doporučuji k takto rozdělené síti vést dokumentaci a pravidelně ji aktualizovat.

3.5.2 Zařízení typu router

V rámci této organizace doporučuji odstranit stávající zařízení typu router a nahradit je serverovým řešením. To znamená nainstalovat služby, které zprostředkují současná zařízení na virtuální stanici. Více k tomuto tématu v kapitole 3.6.1.2 kde je popsán server a virtuální stanice.

3.6 Koncové stanice

3.6.1 Stanice typu server

Doporučuji výměnu serverů, které jsou značně zastaralé jak po hardwarové stránce, tak po stránce operačního systému. Operačnímu systému brzo končí jeho podpora a nový systém na stávajících serverech poběží s obtížemi.

Doporučuji nahradit dva stávající servery jedním, který bude mít dostatečný výkon pro stávající aplikace i pro virtualizaci. Do budoucna díky této investici může škola ušetřit

nemalé peníze za nákup dalších serverů popřípadě dalšího vybavení, které se dá virtualizovat.

3.6.1.1 Hardware

Doporučuji server od firmy HP, u kterého čistá investice do hardwaru činí s DPH necelých 90 000 Kč. Tento server je osazen šesti jádrovým procesor, 64GB RAM, dvěma SSD disky o kapacitě 500GB a dvěma SATA disky o velikosti 2 TB. Pokud by organizace chtěla k tomuto hardwarovému řešení přikoupit i konfiguraci firmwaru, nastavení RAID, instalaci VMware vSphere Hypervisoru, popřípadě jiných služeb měla by počítat s dalšími náklady okolo 10 000 Kč.

K serveru doporučuji připojit záložní zdroj USP, který bude filtrovat přepětí v elektrické síti a v případě výpadku proudu zamezí ztrátě dat z nekorektního vypnutí.

Tab. č. 13: Náklady na nákup serveru

Název	Počet	Cena/kus bez DPH	Cena bez DPH
HP ProLiant ML350 Gen9	1	36 311 Kč	36 311 Kč
Crucial 64GB KIT DDR4 2133MHz CL15 ECC Registered	1	20 915 Kč	20 915 Kč
WD SE RAID Edition 2000GB	2	3 340 Kč	6 680 Kč
Samsung 850 EVO 500GB	2	5 137 Kč	10 274 Kč
		Cena bez DPH	74 180 Kč
		Cena s DPH	89 758 Kč

(Zdroj: Vlastní zpracování)

3.6.1.2 Operační systémy a jejich použití

Doporučuji k tomuto serveru zakoupit tři licence Windows Server Standard 2012 R2. Tyto licence umožní organizaci využít všech 6 jader, virtualizaci pro až 6 další stanic a plně pokryje veškeré funkce používané organizací.

Z první virtuální stanice doporučuji vytvořit zařízení spravující síťový provoz organizace. Doporučuji nainstalovat operační systém Debian nebo Red Hat. V těchto systémech doporučuji nainstalovat aplikace zprostředkující DHCP, DNS a služby

firewall. Firewall doporučuji modifikovat podle pravidel, uvedených v encyklopedii Common Vulnerabilities and Exposures.

Na druhé virtuální stanici doporučuji vytvořit Active Directory a nainstalovat zde Windows Server Update Service, který se stará o instalaci aktualizací. Dále zde doporučuji nainstalovat MSQL server a serverovou část aplikace Bakaláři.

Do třetí virtuální stanice doporučuji škole nainstalovat Windows Backup Server, který bude automaticky spravovat funkci zálohování.

3.6.1.3 Fyzická bezpečnost

Doporučuji jej umístit do místnosti s malou prašností a klimatizací, která bude regulovat teplotu a vlhkost. Zvolená místnost musí být uzamykatelná a nejlépe s alarmem.

3.6.1.4 Licenční stav softwaru a jeho kontrola

V případě, že se škola nerozhodne zakoupit nový server s novými licencemi, doporučuji aktualizovat stávající operační systém Windows Server 2003, kterému končí podpora v půlce července tohoto roku na Windows Server 2012 R2. V rámci této akce je zapotřebí znova nastavit služby Active Directory. Doporučuji správci, který má na starosti servery vytvoření záložního obrazu disků. V případě pádu serveru je zde snadná a jednoduchá obnova. Jedním z možných nástrojů, kterými lze obraz systému vytvořit a následně distribuovat, je program ImageX, který je produktem firmy Microsoft.

Doporučuji zavedení dokumentace aplikací a služeb, které jsou na serveru. Důvodem je evidence a předcházení přečerpání licencí.

3.6.1.5 Další doporučení

K serveru doporučuji přikoupit zařízení NAS, které by zabezpečovalo zálohování a mohlo by zajistit minimalizaci škod při HW selhání serveru. Zařízení NAS by šlo také používat jako FTP server, server pro sdílení souborů, popřípadě media server. Některé NAS zařízení mají vestavěnou službu VPN, takže v případě zavedení kamerového systému lze data nahrávat na NAS a spravovat je odkudkoliv. Hlavní výhodou tohoto zařízení je oproti serveru mnohdy značně jednodušší správa a především nízká spotřeba elektrického proudu.

V situaci, kdyby nebylo zapotřebí ohlížet se na finanční zdroje, bych organizaci doporučil zakoupit zařízení typu QNAP TS-870. Jsem si však vědom, že z důvodu finanční náročnosti nepřipadá toto řešení v úvahu. Proto doporučuji zařízení typu Synology DiskStation DS1515, které také vyhovuje požadavkům organizace. Níže uvádím popis obou zařízení, které připadají v úvahu.

QNAP TS-870

Toto datové úložiště má 8 pozic pro disky 2, 5“, nebo 3, 5“ disky, s podporou až 4 TB na jednu pozici, což umožňuje získat až 32 TB úložného prostoru. Dále podporuje RAID 0, 1, 5, 6, 10 + hot spare disk, 5 + hot spare disk, či 6 + hot spare disk. O samotné fungování úložiště se stará dvoujádrovým procesorem Intel Celeron, který je taktován na 2. 6 GHz. V základu má toto datové úložiště 2 GB RAM, lze ji však rozšířit až na hodnotu 16 GB. Zařízení disponuje funkcemi File Server, FTP Server, Backup Server, Print Server, iTunes Server, Download Station, Media server, či nahráváním i IP kamer. Dále nechybí podpora VMware Ready, Citrix XenServer Ready ani Windows Hyper-V . Rychlost je maximálně 498 MB/s při čtení a 436 MB/s při zápisu (24).

Cena tohoto zařízení bez disků se pohybuje okolo 33 964 Kč včetně DPH.

Obr. č. 12: QNAP TS-870 (24)

Synology DiskStation DS1515

Druhé navrhované datové úložiště je levnější, bez disků stojí okolo 21 538 Kč. Oproti předešlému zařízení má pouze 5 diskových pozic a lze zde umístit pouze 3, 5“ disky. Zařízení podporuje RAID 0, 1, 5, 6, 10 (1+0). Na každou pozici ovšem lze připojit až 6TB disk což umožňuje získat 30 TB úložného prostoru. Datové úložiště disponuje výkonným čtyřjádrovým procesorem taktovaným na frekvenci 2, 4 GHz. V základu je toto datové úložiště osazeno 2GB RAM, čtení tohoto zařízení je 450 MB/s a rychlost zápisu 396 MB/s. Toto zařízení podporuje sdílení souborů (SAMBA, HFS, CIFS), Web server, Databázový server, FTP server, Media server, iTunes. Nechybí zde ani podpora virualizaci VMware, Cytrix, Microsoft Hyper – V, VMware vSphere 5 (25).

Obr. č. 13: Synology DiskStation DS1515 (25)

3.6.2 Koncové stanice uživatelů

3.6.2.1 Hardware

Doporučuji v organizaci povolit užívání pouze koncových stanic vlastněných organizací. Tímto se organizace vyhne prvotní kontrole a konfiguraci zařízení ve

vlastnictví třetích osob. Za následný stav počítače jak fyzický (hardwarový), tak softwarový bude zodpovědný zaměstnanec, který bude mít v užívání danou koncovou stanici. Tuto zodpovědnost podepíše uživatel ve chvíli předání počítače do užívání.

Všechna zařízení musí být nakonfigurována správcem sítě, nebo zodpovědnou osobou.

3.6.2.2 Software

Doporučuji jasně stanovit aplikace, které budou nainstalovány na koncových stanicích uživatelů. Níže uvádím návrh daných aplikací:

- licencovaný operační systém,
- licencovaný kancelářský balík,
- webový prohlížeč Explorer a Firefox,
- multimediální přehrávač, s balíkem kodeků.

3.6.2.2.1 Další povolené aplikace

Po konzultaci se správcem, vedením organizace a následném schválení těmito autoritami, je možné doinstalovat na počítače vybrané stanice i jiný software, který bude licenčně v pořádku. To znamená, že software, je freeware pro použití v organizaci, nebo pro něj škola má zakoupenou licenci. Příklad aplikací:

- GIMP,
- PSPad editor,
- Zoner Calisto 4 ,
- Photo Studio 8 ,
- Pinnacle Studio.

3.6.2.2.2 Zakázané aplikace v síti

Všechny aplikace, které nejsou povoleny, jsou zakázány. Následující aplikace nedoporučuji instalovat v žádném případě i s možností že by organizace – uživatel neporušil licenční podmínky softwaru a byly by schváleny vedením. Důvodem jsou především bezpečnostní mezery, které by instalací mohly v organizaci vzniknout.

- Aplikace podporující službu Torrent (Azureus, BitTorrent, µTorrent ...), nebo aplikace typu DC++, či StrongDC.

- Aplikace sloužící k exploitaci a skenování sítě (Wireshark, NetWorx…).
- Aplikace s shareware licencí.
- Aplikace, pro které organizace nevlastní legální licenci.

Licenční stav softwaru a jeho kontrola

V rámci celé organizace se vyskytuje velké množství koncových stanic. Nikde není kontrolován jejich licenční stav. Proto doporučuji organizaci softwarový audit, který ukáže, jak si celá organizace stojí. Najme-li si organizace na tento audit specializovanou firmu, zaplatí zhruba 250 Kč/počítač což organizace přijde na cca 35 000 Kč (140 počítačů). V případě analyzované organizace bych nevolil volbu interního auditu z důvodu časové náročnosti, nedostatku personálních kapacit a zkušeností.

Částka 35 000 Kč se může zdát být přehnaná, avšak postihy v případě auditu státní organizace a nalezení například nelicencovaného operačního systému Windows mohou mít pro školu katastrofální následky. Konkrétně se jedná o pokutu v řádech deseti až statisíců korun, nákup licencí v plné ceně, trestní stíhání vedení školy a samozřejmě špatnou reklamu celé organizace.

V případě, že se organizace rozhodne neinvestovat do softwarového auditu, další možností je v první řadě napsat dokumentaci (zapotřebí napsat i v případě softwarového auditu) k aplikacím koncových stanic a následně přeinstalovat všechny dostupné stanice softwarem s ověřenou licencí. Následně je důležité zdokumentovat, co je nainstalováno, v jaké verzi a s jakou licencí. Důvodem je prevence přečerpání licencí a odstranění aplikací, které nesplňují licenční podmínky.

V rámci získaných dat, doporučuji aktualizovat všechny stanice, na nichž je nainstalován zastaralý a nepodporovaný operační systém Windows XP, a to minimálně verzí Windows 7.

Doporučuji zavést dokumentaci, která bude popisovat, co má být na PC nainstalované. V rámci této dokumentace by mělo být také uvedeno, kdo je zodpovědný za dohled nad nainstalovanými aplikacemi. Podrobněji je toto téma popsáno v kapitole politika bezpečnosti sítě.

Poslední doporučení v rámci koncových stanic je vytvoření obrazu operačního systému, který lze distribuovat na stanice stejného typu. S tímto obrazem budou počítače vždy po přeinstalování ve stejném stavu a správce se nemusí zdržovat zdlouhavými aktualizacemi, které přicházejí po instalaci nového operačního systému. Jedním z možných nástrojů, kterými lze obraz systému vytvořit a následně jej pak distribuovat dále, je program ImageX, který je produktem firmy Microsoft a který vytváří přesný obraz systému.

3.7 Doporučení politiky zálohování a obnovy dat

3.7.1 Zálohování a obnova – směrnice

V rámci organizace doporučuji zavést politiku zálohování. V kapitole koncové stanice/ servery bylo organizaci doporučeno zakoupení NAS. Díky této technologii bude organizace schopna zabezpečit kvalitní automatizovanou zálohu dat. Doporučuji sepsat směrnici zálohování, která bude popisovat:

- Co se bude zálohovat.
- Odkud a kam se bude zálohovat.
- Jakým způsobem budeme zálohovat.
- Jak často se bude zálohovat.
- Kdo je za tuto činnost zodpovědný.
- Přístup k souborům záloh.
- Kde se evidují zálohy.
- Jak dlouho se budou uchovávat zálohy.

Doporučuji, aby navrhnutá směrnice odkazovala na proces obnovování dat, který je zapotřebí strukturovat analogicky jako směrnici pro vytváření záloh. To znamená:

- Co se bude obnovovat.
- Odkud a kam bude probíhat obnova.
- Jakým způsobem budeme probíhat obnovování.
- Kdo je za tuto činnost zodpovědný.
- Přístup k souborům záloh.

- Jak často budou testovány zálohy.
- Kde se evidují obnovy.

3.7.2 Zálohování a obnova

V rámci návrhu implementace nového serveru a NAS doporučuji zálohovat následovně. Zálohování uživatelských dat a Active Directory doporučuji vytvořit sdílený oddíl o velikosti 1,5 TB, který bude zprostředkován zařízením NAS pracující v RAID 5. Zde bude probíhat automatické zálohování zprostředkované Windows Backup System v plném rozsahu jednou za půl roku a každý měsíc zde proběhnou inkrementální zálohy. Zálohy se budou uchovávat po dobu jednoho roku. Za tyto zálohy bude odpovědný vedoucí pracovník starající se o chod Active Directory. Přístup k tomuto oddílu bude mít pouze správce.

Dále doporučuji vytvořit další 2 diskové oddíly na zařízení NAS v RAID 5, se zrcadlením prvního diskového oddílu na pevný server.

První diskový oddíl bude mít velikost 2 TB a doporučuji na něj zálohovat databáze, data z aplikace Bakaláři, školní dokumenty, obrazy jednotlivých zálohovaných systémů, instalační soubory a licence aplikací. Bude zde probíhat týdenní automatická inkrementální záloha a jednou měsíčně k poslednímu dni v měsíci plná záloha. Zálohování bude řízeno Windows Backup System. Zálohy se budou uchovávat půl roku. Na tento oddíl bude mít přístup pouze správce. Druhý diskový oddíl bude sloužit výhradně pro zaměstnance a hromadnou zálohu dokumentů, či jiného elektronického obsahu. Tomuto disku bych přidělil kapacitu 1 TB s přístupem všech zaměstnanců.

Za zálohy je zodpovědný každý uživatel sám, není-li v dokumentaci napsáno jinak.

V rámci přípravy na pád některého důležitého serveru doporučuji sestavit plán obnovy po havárii a vyzkoušet obnovu systému a důležitých aplikací. Je důležité, aby tento proces byl pečlivě zdokumentován, aby v případě jakékoliv poruchy náprava proběhla v co nejkratším čase a s co nejnižšími náklady. Tento úkol doporučuji svěřit jednomu ze správců sítě. Nejlépe tomu, který se bude starat o provoz NAS.

Doporučuji, aby v rámci zálohování byly všechny zařízení typu server a aktivní prvky připojena k UPS zdroji, který udrží zařízení v chodu i v případě hodinového výpadku proudu. Důvodem je bezpečné stažení dat a jejich uložení.

Celková potřebná disková kapacita pro zvolené NAS řešení je 6 TB. Doporučuji do NAS zakoupit tři 3 TB disky z důvodů nižší ceny za GB a případného budoucího rozšiřování prostoru, v případě že by zde chtěla organizace uchovávat školní fotografie či jiná média. Doporučuji zakupovat vždy disky stejné diskové kapacity pro případ poruchy disku a jeho nahrazení.

3.7.3 Média

Doporučuji v organizaci omezit používání „vlastních“ paměťových úložišť (osobních přenosných HDD, flash pamětí, karet či médií typu CD/DVD) pro zálohování a přenos souborů. Hlavním důvodem je přinášení nechtěného obsahu zvenčí do uzavřené sítě školy. Tento obsah může ohrozit fungování školy, popřípadě porušit integritu dat. Řeč je o obsahu typu malware, rootkit, trojský kůň a jiných, které nevědomě uživatelé mohli stáhnout z internetu. Díky tomuto se v organizaci mohou nacházet „Zombie PC“. To se projevuje sníženým výkonem a také zvýšenou vytížeností celé sítě. Dalším důvodem pro omezení užívání osobních paměťových úložišť, je zmenšení rizika vynášení informací.

Na základě předchozího doporučení, doporučuji škole zakoupit paměťová média, která budou sloužit výhradě pro účely organizace. Těmito účely je myšleno zálohování malých souborů, přenos médií, instalačních nebo konfiguračních souborů mezi jednotlivými zařízeními, popřípadě vytvoření instalačního média. Tato média nemohou být použita pro osobní účely a neměla by být použita ani mimo síť školy. V případě použití mimo síť je zapotřebí médium zformátovat v live systému, popřípadě v operačním systému Linux, aby se předešlo případné nákaze z cizí sítě.

3.8 Doporučení a změny autentizace

3.8.1 Zavedení bezpečnostní politiky hesel

Bezpečností politika hesel je značně opomíjené téma, nejen v této organizaci. Politika hesel by měla být jasně a striktně nastavena a následně dodržována. Z tohoto důvodu

doporučuji nastavit politiku hesel u přihlašování do počítačů, aplikací, které vyžadují hesla a samozřejmě do síťových zařízení. Politika musí být jasně a striktně definována v dokumentu, který bude vytvořen zodpovědnou osobou, která bude dohlížet na její dodržování.

V dokumentu by se měly objevit body:

1. Kdo je zodpovědný za dodržování politiky hesel.

Doporučuji, aby za dodržování hesel byl odpovědný pověřený správce sítě.

2. Koho se zvolená politika týká.

Doporučuji, aby se tato politika týkala všech zaměstnanců a žáků školy.

3. Minimální požadavky na heslo:
    - Heslo nesmí být slovníkovým výrazem.
    - Heslo nesmí obsahovat části jmen, příjmení, přihlašovacích údajů, či název organizace.
    - Jedno heslo nesmí být použito ve více aplikacích najednou.
    - Heslo musí obsahovat minimálně 8 znaků.
    - Heslo musí obsahovat minimálně jedno velké a jedno malé písmeno.
    - Heslo musí obsahovat minimálně jeden speciální znak.
    - Heslo musí být změněno okamžitě po exspiraci.
    - Heslo nesmí obsahovat stejný znak více než 2 krát.
    - Helo, musí uživatel chránit jako utajovanou skutečnost s nejvyšším stupněm utajení a nesmí jej sdílet s jiným uživatelem.

Doporučená doba exspirace hesel podle systému

- Exspirace systémových hesel 2 krát za rok (každých 6 měsíců).
- Exspirace hesel do aplikace Bakaláři jednou za 12 měsíců.
- Exspirace hesel na síťových zařízeních jednou za 6 měsíců.

Doporučuji ve směrnici uvést, že v případě dočasného opuštění pracovní stanice je nutné stanici uzamknout a to například stiskem klávesové zkratky CTRL – ALT – DEL a následně zvolit volbu „Uzamknout stanici“.

Dále v rámci autentizace doporučuji ve směrnici uvést že, administrátor používá administrátorský účet Administrator jen pro správu systému, ne pro své uživatelské aktivity. Pro potřeby uživatelských aktivit užívá jiného účtu se standardním uživatelským nastavením.

Tato opatření nechrání jenom organizace, ale také samotné uživatele, před zneužitím jejich uživatelských účtů. Uživatelé by také měli dodržovat pravidlo, že hesla si nikde nezapisují, ale pamatují si je. V případě že mají více hesel a nejsou schopni si je zapamatovat, lze jim doporučit používání aplikace pro správu hesel jako je například KeePass Password.

V rámci autentizace doporučuji aktualizovat pravidla Active Directory, která se týkají hesel a přístupových práv uživatelů.

3.9 Politika vzděláváni

Vzdělávání ohledně informační bezpečnosti je v této organizaci na velice nízké úrovni. Z tohoto důvodu je zapotřebí zavést systém vzdělávání a proškolování v pravidelném intervalu minimálně jednou za rok.

Doporučuji zavést tři stupně vzdělávání:

3.9.1 Vzdělávání zaměstnanců

Všichni zaměstnanci by měli minimálně jednou za dva roky absolvovat školení bezpečnosti v informačních technologiích. Školení by mělo probíhat každoročně, aby měli všichni zaměstnanci možnost, splnit podmínku být proškolen v této tématice minimálně jednou za dva roky.

Školení by mělo obsahovat tyto body:

- Zásady bezpečné práce s internetem.
- Zásady účinné a aktivní ochrany před virtuálními útoky.

- Zásady práce s hesly.
- Zásady práce se softwarem a základní informace o licenčních právech.
- Zásady bezpečně práce ve školní síti.
- Kde hledat a najít informace o managementu bezpečnosti dané organizace.
- **Zásady ISMS organizace.**

Školení by měl vést člověk zběhlý v problematice, nejlépe také certifikovaný. Výstupem školení bude dokument obsahující témata, která byla probírána v bodech. Dokument by měl být podepsán všemi zúčastněnými. V rámci toho školení by také měli být zaměstnanci proškoleni o fungování managementu bezpečnosti v organizaci. Zaměstnancům, kteří nejsou ve styku s ICT technologiemi, může být školení prominuto vedením organizace.

3.9.2 Vzdělávání správců

Správci by měli projít stejným školením jako ostatní zaměstnanci. Doporučuji u nich však rozšířit vzdělávání v jim blízké problematice a umožnit jim následnou certifikaci. Škola tímto způsobem může motivovat či odměňovat své zaměstnance a navíc získá, zkušenosti, díky kterým si nebude muset najímat externí zaměstnance.

3.9.3 Vzdělávání žáků

V rámci vzdělávání žáků doporučuji rozšířit řád odborné učebny a její provozní řád. Viz příloha číslo 1 a 2. Doporučuji, aby také žáci v rámci vyučování obdrželi informace, které se jich týkají, popřípadě jim mohou být k užitku.

- Zásady bezpečné práce na internetu.
- Zásady účinné a aktivní ochrany před virtuálními útoky.
- Zásady práce s hesly.
- Zásady **ISMS organizace.**

3.10 Doporučení a změny směrnic v dokumentace organizace

V rámci každé organizace by měly být jasně stanoveny dokumenty, směrnice popisující aktuální stav a fungování organizace. Měly by zde být příručky jak pro uživatele, tak pro správce. Některé z nich byly navrhnuty v předchozích kapitolách. Doporučuji, aby

tyto příručky byly napsány zaměstnanci zodpovědnými za konkrétní funkce a následně reevidovány vedením organizace. Tímto škola ušetří náklady, které by musela vynaložit za externí firmu. Navíc zodpovědní zaměstnanci se tímto způsobem vzdělají v problematice, za kterou jsou odpovědni.

3.11 Přínosy managementu bezpečnosti a vyčíslení nákladů

V organizaci, která je nezisková nelze přesně vyčíslit, kdy se daná investice do zabezpečení ICT vrátí, či kdy je výhodná. Lze však říct, co je nutné a nezbytné pro další bezpečné fungování organizace. Změny, které byly v práci navrhnuty, jsou pro tuto organizaci s velkou pravděpodobností dlouhodobého rázu. Důvodem je finanční a technická stránka věci.

V tabulce číslo 13 jsem souhrnně vyčíslil finanční náročnost technického řešení, které jsem doporučil zavést.

Tab. č. 14: Vyčíslení nákladů na technické řešení

Název	Cena
Zavedení managementu pasivní vrstvy	40 000,00 Kč
Server	89 758,00 Kč
NAS	33 964,00 Kč
NAS HDD 3 * 3 TB	9 987,00 Kč
Softwarový audit	30 000,00 Kč
Nákup licencí WIN 7 (1300 Kč/licence)	176 800,00 Kč
Nákup licencí Windows Server 2012 R2	19 680,00 Kč
SUMA	400 189,00 Kč

(Zdroj: Vlastní zpracování)

V případě položek zavedení managementu bezpečnosti pasivní vrstvy, NAS zařízení a licencí operačních systémů Windows 7 je počítáno s rezervou. U zavedení nultého, prvního a druhého stupně ochrany pasivní vrstvy je možné ovlivnění konečné ceny částečnou rekonstrukcí síťové infrastruktury, která má proběhnout. Tyto opatření se totiž zavádějí pro již hotovou síťovou infrastrukturu pasivní vrstvy a náklady na zavedení budou přibližně 20 % z ceny existujícího řešení. Jedná-li se o licence, byly zde

brány v úvahu všechny koncové uživatelské stanice, které škola vlastní. V rámci kalkulace NAS zařízení, bylo počítáno s dražším variantou zařízením, která byla uvedena v textu.

Časová náročnost na zavedení dokumentace je zhruba **540 hodin**. Toto je pouze odhad, záleží na znalostech osoby, která bude dokumentaci vytvářet. Doporučuji škole přistoupit k tvorbě dokumentace následujícím způsobem. Odpovědný zaměstnanec vytvoří dokumentaci, bude ji udržovat v aktuálním stavu a za to obdrží měsíční fixní příplatek ve stanovené výši. Doporučuji příplatek ve výši 500–2000 Kč.

Zdroje školy po odečtení nákladů na platy zaměstnanců a provozní chod školy se pohybují ve výši kolem 11,5 miliónů korun. Tyto zdroje jsou sice součástí financování sportovních aktivit školy, příspěvků na školní výlety, kulturní akce a odměn zaměstnanců. Doporučuji však z tohoto zdroje navýšit částku, která je nyní investována do ICT školy o 100 000 až 300 000 Kč ročně. Tato částka by měla být s uvážením investována do informačních technologií a bezpečnosti, a to do hardwaru, softwaru, směrnic, nebo školení zaměstnanců, popřípadě žáků.

Suma, kterou jsem navrhnul výše, není malá. Vedení organizace si však musí uvědomit, že v případě problémů by mohla přijít o nemalé finanční prostředky a o dobrou pověst, kterou organizace má. Jako příklad, lze uvést kontrolu softwaru, softwarový audit odpovědným státním orgánem a případný nález nelegálního softwaru.

Protipirátská organizace BSA uvádí, že průměrné odškodné za používání nelicencovaného softwaru se v Česku pohybuje ve výši 300 000 Kč. K tomu je zapotřebí započíst sumu za nákup licencí za plnou cenu a jednorázové náklady ve výši 500 000 Kč jsou na světě. Nesmíme také zapomenout na soudní stíhání vedení organizace, které nemá ponětí, co se serverech a pracovních stanicích využívaných zaměstnanci a žáky děje. To je také důvod proč by měl ustanovit osobu, která je zodpovědná za dohlížení nad touto činností.

Suma 500 000 Kč, do které by se škola v případě výše uvedené situace dostala, odpovídá dvou až pětileté investici do ICT. Proto z mého pohledu doporučuji raději investovat zvolenou sumu peněz do vlastní organizace, než riskovat nepříznivé následky jako jsou placení pokut a trestní stíhání.

V tabulce číslo 14 uvádím přehledně v tabulce vyobrazené výhody a nevýhody zavedení managementu bezpečnosti.

Tab. č. 15: Výhody a nevýhody managementu bezpečnosti

VÝHODY	NEVÝHODY
Ujasnění procesů a funkcí	Zvýšené náklady na vzdělávání zaměstnanců
Bezpečnější provoz školy	Časová náročnost zavádění
Získání povědomí o bezpečnosti ICT	
Bezpečné uchovávání dat	
Zvýšení konkurenceschopnosti	
Možné vyhnutí se sankcím za porušení licenčních podmínek	
Případná certifikace	

(Zdroj: Vlastní zpracování)

ZÁVĚR

Reálným výstupem mé diplomové práce jsou návrhy na zavedení bezpečnostních prvků bezpečnosti ICT, které by vedení školy, správcům a možná i veřejnosti měly sloužit jako důvod k zamyšlení a hlavně důvod k implementaci konkrétních opatření nejen v analyzované organizaci. V případě, že mé návrhy budou realizovány, pevně věřím, že mohou přispět k lepšímu vedení a fungování celé organizace. Doufám v to, že tyto návrhy pomohou celkově zvýšit povědomí o bezpečnosti v oblasti ICT technologií a poskytnou vodítko pro zlepšování.

V první části jsem popsal teoretická východiska nezbytná pro porozumění této práci. Snažil jsem se čtenáři přiblížit management bezpečnosti ICT v co nejširším slova smyslu. Nejen formou norem a obsáhlých ustanovení, ale také za pomoci příkladů.

V druhé části mé diplomové práce jsem se zabýval analýzou zvolené organizace. Čtenáři jsem podal náhled na aktuální stav organizace. Z tohoto náhledu vyplynulo, že škola má značné problémy týkající se vedení dokumentace bezpečnosti procesů ICT. Dále bylo zjištěno, že jsou zde nedostatky v HW řešení.

V praktické části, která vycházela z analýzy stavu organizace, byla provedena analýza rizik. Na základě analýzy rizik jsem formuloval doporučení týkající se hlavních problémů organizace. Mezi hlavní doporučení patřilo zavedení managementu bezpečnosti pasivní vrstvy, obnova serverového řešení, které obsahovalo také zařízení typu NAS. V rámci těchto doporučení byly doporučeny směrnice dokumentující zálohování a obnovu dat. Dále jsem učinil návrh týkající se autentizace a autorizace uživatelů.

V práci jsem se nezabýval všemi aspekty týkající se bezpečnosti ICT. Důvodem byla rozsáhlost těchto témat. Zabýval jsem se především nejzávažnějšími problémy, které organizace měla z mého pohledu a z pohledu analýzy rizik, jež byla provedena ve třetí části mé práce.

Cílem mé diplomové práce bylo navrhnout změny, které organizaci pomohou zlepšit její fungování a bezpečný chod v rámci managementu ICT. Pevně věřím, že tento cíl jsem splnil, a že mnou podané návrhy škole pomohou ke zlepšení stávajícího stavu.

SEZNAM POUŽITÉ LITERATURY

(1) MLÁDKOVÁ, L. a P. JEDINÁK. *Management*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2009, 273 s. ISBN 978-80-7380-230-1.

(2) ŠTALMACH, P. a J. ŠEDIVÝ. *Management bezpečnosti*. Praha: CEVRO Institut, 2012. 124 s. ISBN 978-80-87125-19-9.

(3) DOUCEK, P. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2. přepracované vydání. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.

(4) ONDRÁK, V., P. SEDLÁK a V. MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013. 377 s. ISBN 978-80-7204-872-4.

(5) *AXELOS. ITIL V3 Glossary of terms, Definitions and Acronyms* [online]. 2007 [cit. 2015-03-22]. Dostupné z: *http://www.best-management-practice.com/gempdf/itil_glossary_v3_1_24.pdf*

(6) KOUDELKA, C. a V. VRÁNA. *Rizika a jejich analýza: Fakulta elektrotechniky a informatiky* [online]. 2006 [cit. 2015-04-23]. Dostupné z: *http://fei1.vsb.cz/kat420/vyuka/Magisterske%20nav/prednasky/web/RIZIKA.pdf*

(7) ISO/IEC 27000:2009. *Information technology — Security techniques — Information security management systems — Overview and vocabulary*. Switzerland: ISO/IEC, 2009. 26 p.

(8) MATUSÍK, J. *Management informační bezpečnosti* [přednáška]. Brno: VUT v Brně, Fakulta podnikatelská, 6. 10. 2014.

(9) ISO/IEC 27002:2005. *Information technology — Security techniques — Code of practice for information security management*. Switzerland: ISO/IEC, 2005. 128p.

(10) ČSN ISO/IEC 27000:2014. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. 31 s. Třídící znak 369790.

(11) SOSINSKY, B. *Mistrovství – počítačové sítě*. Brno: Computer Press, 2010. 840 s. ISBN 978-80-251-3363-7.

(12) What is OSI Model. *Researcher's Blog* [online]. 2013 [cit. 2015-04-15]. Dostupné z: http://clean-clouds.com/2013/05/what-is-osi-model/

(13) KUROSE, F. a K. ROSS. *Počítačové sítě*. Brno: Computer Press, 2014, 622 s. ISBN 978-80-251-3825-0.

(14) Jaký je rozdíl mezi malwarem a virem. SPECTOR, Lincoln a Pavel KREUZIGER. *PCWorld* [online]. 2013 [cit. 2015-04-26]. Dostupné z: http://pcworld.cz/software/jaky-je-rozdil-mezi-malwarem-46659

(15) Škodlivý software (MALWARE). *INNET | VŠB – Technická univerzita Ostrava* [online]. 2012 [cit. 2015-04-26]. Dostupné z: http://idoc.vsb.cz/cs/okruhy/cit/pc/bezpecnost/spyware

(16) Network-attached storage (NAS). *Tech Targer* [online]. 2014 [cit. 2015-04-26]. Dostupné z: http://searchstorage.techtarget.com/definition/network-attached-storage

(17) TATE, J., B. Cartweight a J. Cronin. *IBM SAN Survival Guide*. 2nd ed. San Jose, CA: IBM International Technical Support Organization, 2003. 622 p. ISBN 0738454338

(18) Wireless N Gigabit Router DIR-655. *D-Link* [online]. 2007 [cit. 2015-05-15]. Dostupné z: http://www.dlink.com/cz/cs/home-solutions/connect/routers/dir-655-wireless-n-gigabit-router

(19) SMC Networks EZ Switch SMCGS24C-Smart a rozdělení gigabitových přepínačů do čtyř skupin. KLAŠKA, L. *Svět sítí* [online]. 2006 [cit. 2015-05-15]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=SMC-Networks-EZ-Switch-SMCGS24C-Smart-a-rozdeleni-gigabitovych-prepinacu-do-ctyr-skupin-1082006

(20) 24portový gigabitový řízený switch L2 s 4 sloty Combo SFP TL-SG3424. *TP-Link* [online]. 2014 [cit. 2015-05-15]. Dostupné z: http://cz.tp-link.com/products/details/?model=TL-SG3424

(21) 24-Port Gigabit Unmanaged Desktop Switch DGS-1024D. *D-Link* [online]. 2006 [cit. 2015-05-15]. Dostupné z: http://www.dlink.com/uk/en/business-solutions/switching/unmanaged-switches/rackmount/dgs-1024d-24-port-copper-gigabit-switch

(22) MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY. *Statistická ročenka školství: výkonové ukazatele* [online]. 2015 [cit. 2015-02-18]. Dostupné z: http://toiler.uiv.cz/rocenka/rocenka.asp

(23) VLADIMÍR, Hulík. MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY. *Vývojová ročenka školství 2004/05–2013/14* [online]. 2014 [cit. 2015-02-18]. Dostupné z: http://www.msmt.cz/file/34263/download/

(24) QNAP TS-870 Pro. *QNAP* [online]. 2013 [cit. 2015-05-15]. Dostupné z: https://www.qnap.com/i/en/product/model.php?II=108

(25) Synology DiskStation DS1515. *Synology* [online]. 2014 [cit. 2015-05-15]. Dostupné z: https://www.synology.com/en-us/products/DS1515

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

CIFS – Common Internet File System

CISO – Chief Information Security Officer

CLI – Command Line Interface

COBIT – Control Objectives for Information and Related Technology

ČSN – Česká Státní Norma

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

FTP – File Transfer Protocol

HFS – HTTP File Server

HTTP – Hyper Text Transfer Protocol

HTTPS – Hyper Text Transfer Protocol Secure

HW – Hardware

ICT – Information and Communication Technologies

IDS – Intrusion Detection Systems

IEC – International Electrotechnical Commission

IP – Internet Protocol

IPS – Intrusion-Prevention Systems

ISMS – Information Security Management System

ISO – International Organization for Standardization

ITIL - Information Technology Infrastructure Library

LAN – Local Area Network

NAS – Network Attached Storage

NAT – Network Address Translation

OS – Operating System

OSI – Open Systems Interconnection

P2P – Peer-to-peer (network)

PDF – Portable Document Format

QoS – Quality of Service

RAID – Redundant Array of Inexpensive/Independent Disks

RAM – Random Access Memory

SAN – Storage Area Network

SFP – Small Form-factor Pluggable

SMB – Server Message Block

SMTP – Simple Mail Transfer Protocol

SQL – Structured Query Language

SSD – Solid-State Drive

SW – Software

UPS – Universal Power Supply

UTP – Unshielded Twisted Pair

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

WAN – Wide Area Network

SEZNAM GRAFŮ

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHY

Příloha č. 1 : Osnova poučení žáků

Základní škola ..... ve .....

PROVOZNÍ ŘÁD

Učebny výpočetní techniky vybavené počítači

1. Všeobecné ustanovení

   1.1. Učebna výpočetní techniky (dále UVT) vybavena počítači je určena

   - Především pro potřeby výuky žáků základní školy.
   - Pro zpracování dat a údajů pracovníků škol.
   - V době mimo vyučování pak slouží k rozvoji zájmu o VT žáků a vzdělávání dospělých ve spolupráci s organizací.

   1.2. Provozní řád UVT obsahuje:

   - Vymezení odpovědnosti za provoz učebny.
   - Zajištění bezpečnosti a hygieny provozu učebny.
   - Zásady manipulace s prostředky, tvořícími vybavení učebny.
   - Závěrečné ustanovení.

2. Vymezení odpovědnosti za provoz učebny

   2.1. Řízení UVT byl vedením školy pověřen _____, který odpovídá za celkový provoz.

Stanoví zejména:

- Rozvrh provozu UVT v době vyučování a v době mimo vyučování.
- Kontroluje provoz a dodržování Provozního řádu.
- Zajišťuje údržbu a opravy zařízení učeben.

2.2. Vstup do UVT mají povolen:

- určení vyučující dle rozvrhu výuky,
- žáci v doprovodu odpovědných pracovníků,
- ředitel školy,

- účastníci kurzu VZ,
- školník, údržbář, uklízečka,
- další osoby se souhlasem a doprovodem pracovníka pověřeného vedením UVT.

2.3. Klíče od UVT má vedoucí pracoviště, učitelé VT, ředitel školy, uklízečka a sekretariát

2.4. Každý pracovník přebírá vstupem do učebny plnou zodpovědnost za vybavení, provoz a dodržování bezpečnosti provozu a ochranu zdraví

Odpovědný pracovník po skončení práce je povinen:

- Vypnout po skončení práce všechna elektrická zařízení
- Dbát pořádku a čistoty na všech pracovištích i v celé učebně
- Ohlásit vedoucím UVT všechny poruchy a zdokumentovat je
- V učebně musí být při odchodu uzavřena okna, zhasnuta světla. Učebna musí být vždy řádně uzamčena

3. Pravidla vlastního provozu

3.1. Za dodržování všech pravidel odpovídá učitel, který žáky vyučuje, nebo má UVT dozor

3.2. V učebně platí řád školy. Mimo to je UVT zakázáno pít, kouřit a manipulovat s otevřeným ohněm.

3.3. Jsou zakázány jakékoliv zásahy do sestavy počítačů a el. Sítě učebny

3.4. Povinností všech je dodržovat v UVT čistotu a pořádek

3.5. S počítači mohou manipulovat pouze osoby poučené a obsluhy znalé. Při obsluze musí být dodrženy předepsané postupy.

3.6. Všechny poruchy je třeba ihned hlásit správci učebny. Ten zajišťuje odbornou opravu.

3.7. Seznámení všech uživatelů UVT s tímto „Provozním řádem“ bude pořádáno 1 * ročně

3.8. Nedbalost nebo opakované porušovaní „Provozního řádu“ bude vedením školy trestáno ve smyslu zákonných ustanovení

Tento provozní řád nabývá platnost dne _____

Podpis ředitele školy podpis správce učebny

Příloha č. 2 : Řád odborné učebny

Řád odborné učebny výpočetní techniky

Směrnice vydaná ředitelem školy

1. Žáci se shromáždí před učebnou **1 minutu** před zvoněním – přestávku tráví ve své kmenové třídě.
2. Do učebny žáci vstupují pomalu, kulturně a pouze se svolením vyučujícího. Pozor na kabeláž monitorů v řadě „za Vámi“.
3. Aktovky žáci odkládají do prostoru pod umyvadlo. **Je zakázáno chodit s aktovkou mezi počítače.**
4. Je naprosto nepřípustné přidávat do učebny židličky z jiných učeben v případě většího počtu žáků.
5. Jakékoliv závady hlásí žák učiteli (např. chybějící nebo nefunkční součástky či nefunkční programy).
6. V případě požáru nebo úrazu el. proudem je nutné okamžitě vypnout hlavní jističe el. proudu a informovat vyučujícího.
7. Žákovské počítače se mezi jednotlivými hodinami nevypínají, pouze se odhlaste.
8. Dataprojektor vypínejte vždy po každé hodině. V případě domluvy s vyučujícím další hodiny použijte režim MUTE.
9. **Vyučující poslední hodiny daného dne zajistí** vypnutí žákovských počítačů,vypnutí dataprojektoru a reprobeden, zavření oken, smazání tabule a vrácení klíče zpět na sekretariát. Židličky se nezvedají, pouze se srovnají. (viz rozvrh učebny ve sborovně)
10. Učitelský počítač a doménový server se **NIKDY NEVYPÍNAJÍ.** Pouze se odhlaste. Žáci mají přísný zákaz práce na těchto počítačích.
11. Obsluha klimatizace není dovolena. Je nastavena na 22°C což je optimální teplota kdy není ani horko, ani nedochází k nemocem z nachlazení. V případě nutnosti však obsluhu provádí pouze vyučující a nastavení po ukončení výuky uvede do původního stavu.
12. V učebně je zakázáno:
    - jíst a pít,
    - zapínat, restartovat a vypínat počítače bez vědomí vyučujícího,
    - instalovat programy,
    - spouštět programy bez svolení učitele,
    - manipulovat s elektrickými kabely a jiným technickým vybavením, manipulovat s kabeláží na zadní straně počítače,
    - vkládat do počítače paměťová média bez vědomí učitele (pokud to není součástí výuky)
    - sahat na klávesnici a myš špinavýma rukama,
    - opouštět pracovní místo,
    - brát sluchátka ze stojanu bez vědomí vyučujícího, sluchátka se opět vracejí na své místo.

Ve _____ dne XX.YY.ZZZZ Jméno ředitele